Qualys. Consulting Edition

Delivered by ELEVATE

Scan Results

February 20, 2021

Report Summary

User Name:	Sebastian Austin
Login Name:	
Company:	Elevate Consulting
User Role:	Manager
Address:	1172 S. DIXIE HWY, SUITE 311
City:	Coral Gables
State:	Florida
Zip:	33146
Country:	United States of America
Created:	02/20/2021 at 23:16:02 (GMT-0500)
Client:	Elevate Consult
Launch Date:	02/20/2021 at 00:35:18 (GMT-0500)
Active Hosts:	35
Total Hosts:	39
Type:	Scheduled
Status:	Finished
Reference:	scan/1613799318.14862
Scanner Appliances:	ACOSTA (Scanner 12.2.62-1, Vulnerability Signatures 2.5.112-3)
Duration:	01:36:32
Title:	Acosta Internal HQ-DR-QA including DB
Asset Groups:	Acosta Internal Production -DB-, Acosta Internal DR & QA (no DB), Acosta Internal DR & QA -DB-, Acosta Internal Production (no DB)
IPs:	172.16.1.1, 172.16.1.12-172.16.1.14, 172.16.1.80, 172.16.1.253-172.16.1.254, 172.16.10.5, 172.16.10.22, 172.16.30.15, 172.16.30.20-172.16.30.22, 172.16.50.90, 172.16.50.100-172.16.50.102, 172.17.1.1, 172.17.1.15-172.17.1.17, 172.17.1.80, 172.17.1.253-172.17.1.254, 172.17.10.5, 172.17.10.20-172.17.10.22, 172.17.20.20-172.17.20.23, 172.17.30.15, 172.17.30.20-172.17.30.22, 172.17.50.100-172.17.50.102
Excluded IPs:	-
Options Profile:	Combined Profiles

Summary of Vulnerabilities

Vulnerabilities Total	1823	Security Risk (Avg)	🟥🟥□□□ 1.8

by Severity

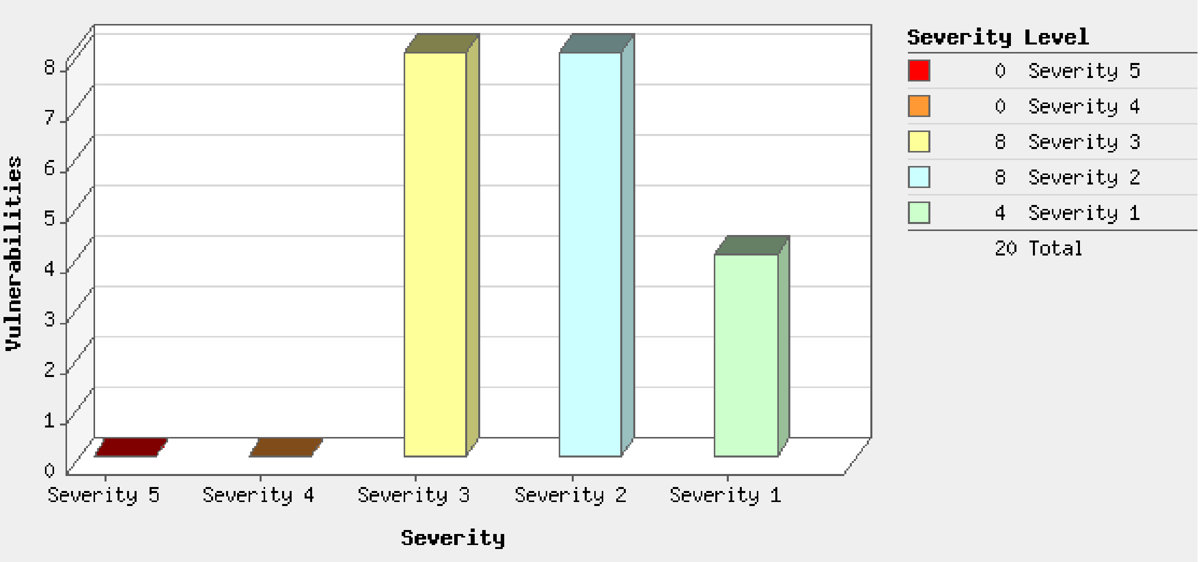
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	12	0	12
3	8	47	41	96
2	8	12	206	226
1	4	12	1473	1489
Total	20	83	1720	1823

5 Biggest Categories

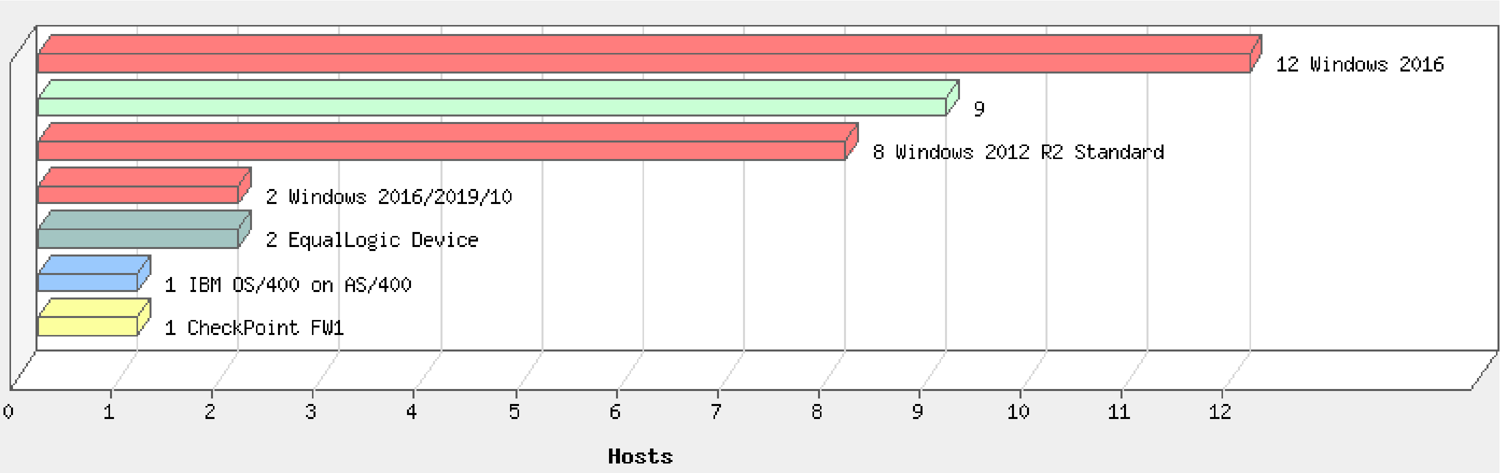
Category	Confirmed	Potential	Information Gathered	Total
General remote services	13	64	522	599
Information gathering	0	3	495	498
CGI	0	4	207	211
Web server	1	2	186	189

Category	Confirmed	Potential	Information Gathered	Total
TCP/IP	0	0	186	186
Total	14	73	1596	1683

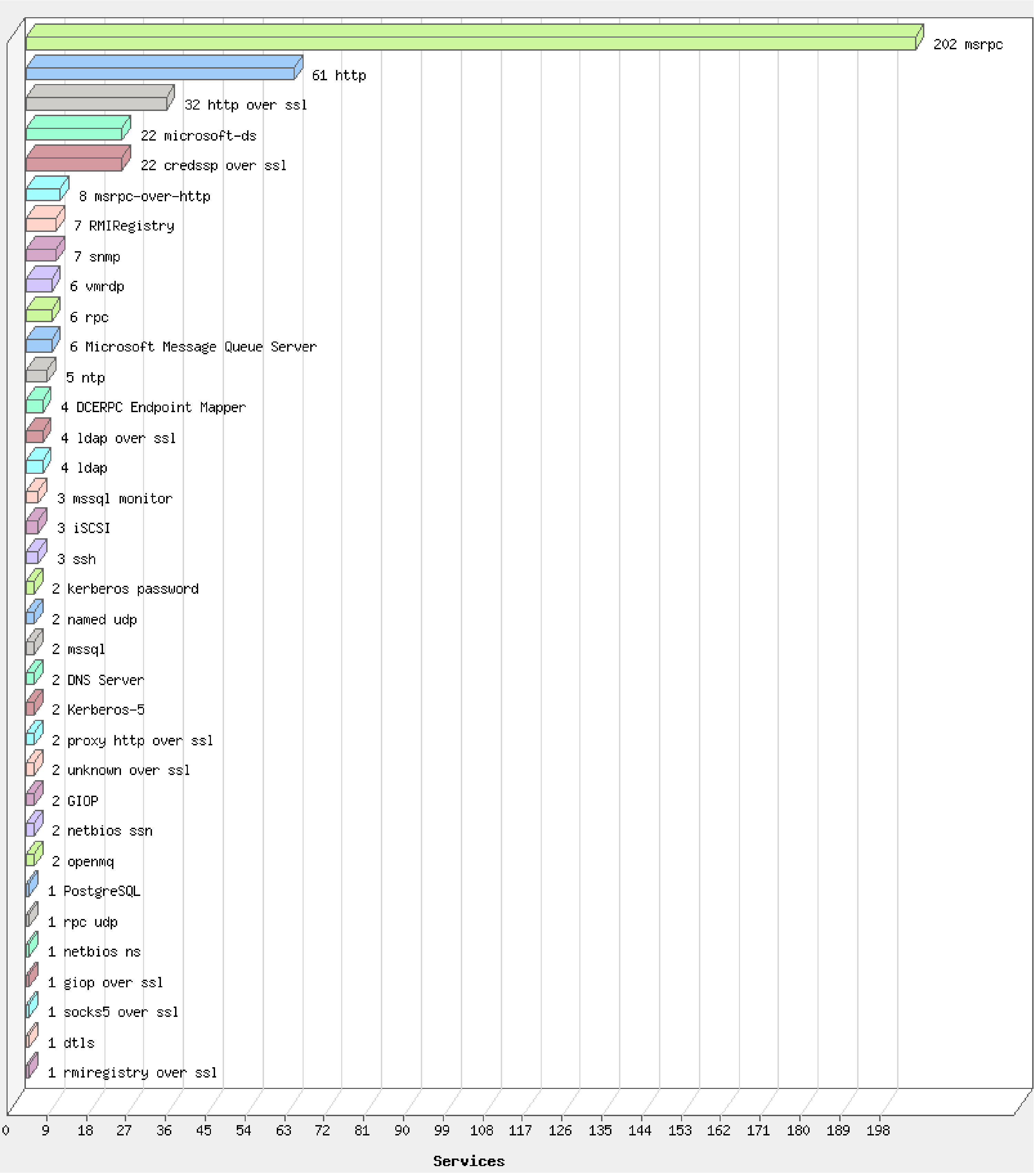
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

172.16.1.1 (-, -)

Information Gathered (6)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.1.1	No registered hostname

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to

perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 302 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 05:41:41 GMT

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
UDP	123	0:00:19
UDP	1812	0:00:07

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
1812	radius	RADIUS	unknown

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)

UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 456	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	05:42:49 GMT
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 61466	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 31335	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 9	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1978	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1027	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7111	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable
Unreachable (type=3 code=3)	UDP Port 445	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 27444	Port Unreachable
Time Exceeded (type=11 code=0)	(Various)	Time Exceeded

■□□□□ 1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

172.16.1.12 (host2.enterate.com, HOST2) Windows 2016

Vulnerabilities (2)

■■■□□ 3 Unauthenticated/Open Web Proxy Detected port 8014/tcp over SSL

QID:	62002
Category:	Proxy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Users with unauthorized internet access can connect to arbitrary services using the HTTP protocol via this proxy.

IMPACT:
Successful exploitation may allow unauthorized users to browse the Internet with your IP address , your Intranet and Web server. This may also be exploited to scan non-http services inside your firewall.

SOLUTION:
Reconfigure your proxy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET http://172.16.1.90:41493/ HTTP/1.0



The Following Adressing Schemes Are Supported:
http://ip4_address
https://ip4_address
```

■□□□□ 1 SSL/TLS Server supports TLSv1.1 port 3389/tcp over SSL

QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/22/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some

vendor implementations of TLSv1.1 have weaknesses which may be exploitable.
This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

IMPACT:

Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:

Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1_1

If the test is successful, then the target support TLSv1.1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.1 is supported

Potential Vulnerabilities (4)

■■■■□ 4 Potential TCP Backdoor

QID:	1004
Category:	Backdoors and trojan horses
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/04/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

There are known backdoors that use specific port numbers. At least one of these ports was found open on this host. This may indicate the presence of a backdoor; however, it's also possible that this port is being used by a legitimate service, such as a Unix or Windows RPC.

IMPACT:

If a backdoor is present on your system, then unauthorized users can log in to your system undetected, execute unauthorized commands, and leave the host vulnerable to other unauthorized users. Malicious users may also use your host to access other hosts and perform a coordinated Denial of Service attack.
Some well-known backdoors are "BackOrifice", "Netbus" and "Netspy". You should be able to find more information on these backdoors on the CERT Coordination Center's Web site (www.cert.org) (http://www.cert.org).

SOLUTION:

Call a security specialist and test the host for backdoors. If a backdoor is found, then the host may need to be re-installed.

COMPLIANCE:

Type: CobIT
Section: DS5.9
Description: Malicious Software Prevention, Detection and Correction
Ensure that preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from Malware (viruses, worms, spyware, spam, internally developed fraudulent software, etc.).

Type: HIPAA
Section: 164.306 and 164.312
Description: Insuring that Malware is not present on hosts addresses section(s) 164.306 and 164.312 requirements for securing critical system files and services and insuring system integrity.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The tcp port 5000 is open, it may indicate the presence of a "Socket23" backdoor.

■■■□□ 3 Apache Tomcat HTTP/2 Request Header Mix-Up Vulnerability

QID:	12375
Category:	CGI
CVE ID:	CVE-2020-17527
Vendor Reference:	Apache Tomcat 8.5.60, Apache Tomcat 9.0.40
Bugtraq ID:	-
Service Modified:	12/10/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
Affected by following vulnerability:
CVE-2020-17527 : Apache Tomcat could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream.
Affected Versions:
Apache Tomcat 8.5.0 to 8.5.59
Apache Tomcat 9.0.0-M1 to 9.0.39
QID Detection Logic (Unauthenticated):
The QID checks for vulnerable version by sending a GET /QUALYS13827 HTTP/1.0 request which helps in retrieving the installed version of Apache Tomcat in the banner of the response.

IMPACT:

Successful exploitation would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.

SOLUTION:

Upgrade to the Apache Tomcat 8.5.60, 9.0.40 or to the latest version of Apache Tomcat. Please refer to Apache Tomcat (http://tomcat.apache.org/index.html).
Workaround:- Disable support for the application/xml content type
- Apply security fix available in source code form (https://svn.apache.org/repos/asf/axis/axis2/java/core/security/secfix-cve-2010-1632) until a fixed version is available.
Detailed information on applying the workarounds can be found at Apache Axis advisory (https://svn.apache.org/repos/asf/axis/axis2/java/core/security/CVE-2010-1632.pdf).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Tomcat 8.5.60 (http://tomcat.apache.org/security-8.html)
Apache Tomcat 9.0.40 (http://tomcat.apache.org/security-9.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Apache Tomcat detected on port 8015.
<h3>Apache Tomcat/9.0.37</h3>Vulnerable version of Apache Tomcat detected on port 8029.

■■■□□ 3 OpenSSL Raccoon Attack Vulnerability(20200909)

QID:	38796
Category:	General remote services
CVE ID:	CVE-2020-1968
Vendor Reference:	20200909
Bugtraq ID:	-
Service Modified:	09/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSL is a commercial-grade, full-featured, open source toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, and provides a full-strength, general purpose cryptography library.
CVE-2020-1968: Vulnerability present in the TLS specification
Affected Versions:
OpenSSL 1.0.2-1.0.2v
QID Detection Logic:(Unauthenticated)
This QID matches vulnerable versions based on the exposed banner information.

IMPACT:

Successful exploitation allows an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite.

SOLUTION:

The vendor has released a patch. Fixed in OpenSSL 1.0.2w and 1.1.1 is not vulnerable. For more information please visit advisory (https://www.openssl.org/news/secadv/20200909.txt).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
20200909 (https://www.openssl.org/news/secadv/20200909.txt)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable OpenSSL version detected on port 8014 over TCP - Apache/2.4.41 (Win32) OpenSSL/1.0.2uVulnerable OpenSSL version detected on port 8015 over TCP -
Date: Sat, 20 Feb 2021 05:46:53 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0
Connection: close

■□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (110)

■■■□□ 3 Content-Security-Policy HTTP Security Header Not Detected port 8016/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given

page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8016.
GET / HTTP/1.0
Host: host2.enterate.com:8016

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 8016/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8016.
GET / HTTP/1.0
Host: host2.enterate.com:8016

3 Content-Security-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Content-Security-Policy HTTP Header missing on port 8014.
GET / HTTP/1.0
Host: host2.enterate.com:8014
```

3 HTTP Public-Key-Pins Security Header Not Detected port 8014/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8014.
GET / HTTP/1.0
Host: host2.enterate.com:8014

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	

Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U4110:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

■■□□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0	135			
DCOM OXID Resolver	0.0	135			
DCOM Remote Activation	0.0	135			
DCOM System Activator	0.0	135, 49703			
Microsoft Cluster Server API	2.0	49720			
Microsoft Distributed Transaction Coordinator	1.0	50203			
Microsoft Local Security Architecture	0.0	49713, 49676			
Microsoft LSA DS Access	0.0	49713, 49676			
Microsoft Network Logon	1.0	49713, 49676			
Microsoft Registry	1.0				\PIPE\winreg
Microsoft Scheduler Control Service	1.0	49703			\PIPE\atsvc
Microsoft Security Account Manager	1.0	49713, 49676			\pipe\lsass
Microsoft Service Control Service	2.0	49711			
Microsoft Task Scheduler	1.0	49703			\PIPE\atsvc
MS Wbem Transport IEnumWbemClassObject	0.0	49703			
MS Wbem Transport IWbemLevel1Login	0.0	49703			
MS Wbem Transport IWbemObjectSink	0.0	49703			

MS Wbem Transport IWbemServices	0.0	49703	
WinHttp Auto-Proxy Service	5.1		\PIPE\W32TIME_ALT
(Unknown Service)	1.0	135	
(Unknown Service)	1.0	49713, 49676	
(Unknown Service)	0.0	49703	
(Unknown Service)	0.0	135	
(Unknown Service)	1.0	49703	
(Unknown Service)	2.0	135	
(Unknown Service)	1.0	49703	\PIPE\atsvc
(Unknown Service)	4.0	49703	
(Unknown Service)	2.0	49703	\PIPE\atsvc
(Unknown Service)	1.0	49703	\pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0	49703	\pipe\LSM_API_service, \pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0	49669	
(Unknown Service)	1.0	49669	\PIPE\InitShutdown
(Unknown Service)	0.0	49713, 49676	
(Unknown Service)	0.0	49713, 49676	\pipe\lsass
(Unknown Service)	2.0	49713, 49676	\pipe\lsass
(Unknown Service)	1.0	49713, 49676	\pipe\lsass
(Unknown Service)	1.0		\pipe\LSM_API_service
(Unknown Service)	0.0		\pipe\LSM_API_service
Event log TCPIP	1.0	49670	\pipe\eventlog
DHCP Client LRPC Endpoint	1.0		\pipe\eventlog
RemoteRegistry Perflib Interface	1.0		\PIPE\winreg
DfsDs service	1.0		\PIPE\wkssvc
Remote Fw APIs	1.0	49707	

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 135, the host's uptime is 3 days, 10 hours, and 7 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

■■□□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 8016/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8016 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8015/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8015 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8029/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 8029 port.GET / HTTP/1.1
```

▮▮▯▯▯ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.1.12	host2.enterate.com

1 Microsoft SQL Server Instances Enumerated

QID:	19145
Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/24/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Microsoft SQL Server instances from the target Windows machine are enumerated.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Name: ARCSERVE_APP
 Port: 53596
 IsCluster: No
 Version: 12.0.5000.0
```

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2178,2180-2512,2514-2701,
2703-3342,3344-3388,3390-4999,5004-5630,5632-5984,5986-6128,6130-6599,
6601-7787,7789-8013,8017-8028,8030-8567,8569-8957,8959-9679,9681-15001,
15004-42423,42425-47000,47002-49668,49671-49675,49677-49702,49704-49706,
49708-49710,49712,49714-49719,49721-49890,49892-50202,50204-59766,59768-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2839 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:24:26 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
host2.enterate.com	NTLM DNS
host2.enterate.com	FQDN
HOST2	MSSQL Monitor
HOST2	NTLM NetBIOS

1 Java Remote Method Invocation Detected

QID:	45186
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/23/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Java Remote Method Invocation or Java RMI, is a mechanism that allows one to invoke a method on an object that exists in another address space.
Java RMI is running on target host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Service name: Java RMI is running  on TCP port 8568.
Service name: Java RMI is running  on TCP port 9680.
```

1 OpenSSL (Open Source toolkit for SSL/TLS) Detected

QID:	45222
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	07/07/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSL is an open-source implementation of the SSL and TLS protocols. OpenSSL is based on SSLeay.
Qualys detected OpenSSL on the host. Please note that in remote detections, security patches may be backported and the displayed version number may not show the correct patch level.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
OpenSSL detected on port 8014 over TCP - Apache/2.4.41 (Win32) OpenSSL/1.0.2uOpenSSL detected on port 8015 over TCP -
Date: Sat, 20 Feb 2021 05:46:53 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0
Connection: close
```

▮▯▯▯▯ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:

Microsoft recommends users to update to latest SMB versions and stop using SMBv1.

Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

1 Apache Tomcat Server Detected

QID:	45387
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Apache Tomcat
Bugtraq ID:	-
Service Modified:	07/06/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
QID Detection Logic (authenticated):
Operating System:Linux
The QID checks for running tomcat servers. The version is extracted from the catalina.jar using "unzip -p" command.
Note:unzip is needed for successful detection.

IMPACT:
NA

SOLUTION:
NA

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Apache Tomcat Server Detected on port: 8015
>Apache Tomcat/9.0.37</h3>Apache Tomcat Server Detected on port: 8029
```

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:01:18
TCP	443	0:04:00
TCP	2179	0:00:45
TCP	3343	0:07:32
TCP	3389	0:00:58
TCP	5000	0:02:10
TCP	5001	0:02:46
TCP	5002	0:02:09
TCP	5003	0:02:09
TCP	5985	0:27:01
TCP	6600	0:02:45
TCP	7788	0:00:33
TCP	8014	1:26:13
TCP	8015	1:15:07
TCP	8016	0:41:09
TCP	8029	0:39:03
TCP	8568	0:04:27
TCP	8958	0:04:14
TCP	9680	0:04:31
TCP	15002	0:06:34
TCP	15003	0:00:32
TCP	47001	0:27:00
TCP	49669	0:05:05
TCP	49670	0:05:12
TCP	49676	0:05:05
TCP	49703	0:05:26
TCP	49707	0:05:05
TCP	49711	0:05:05
TCP	49713	0:05:05
TCP	49720	0:05:05
TCP	49891	0:02:05
TCP	50203	0:05:07
TCP	53596	0:00:36
TCP	59767	0:02:47
UDP	1434	0:00:21

■□□□□ 1 Java RMI Distributed Garbage-Collection Service Detected

QID:	48074
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/13/2020

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Java RMI services can be exposed over network using TCP sockets. Every RMI service is identified by an object number.
Garbage-Collection Service (2 - DGC_ID) is detected on remote RMI service.
QID Detection Logic(Unauthenticated):
This QID sends a Java DGC RMI payload to the remote service.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Java RMI Distributed Garbage-Collection Service Detected on port 8568
Java RMI Distributed Garbage-Collection Service Detected on port 9680
```

1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Microsoft Server Message Block (SMBv3) Compression Disabled

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
1434	ms-sql-m	Microsoft-SQL-Monitor	mssql monitor

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
443	https	http protocol over TLS/SSL	unknown	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
2179	vmrdp	Microsoft RDP for virtual machines	VMRDP	
3343	ms-cluster-net	MS Cluster Net	unknown	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5000	Socket23	backdoor commplex-main	unknown	
5001	commplex-link	commplex-link	unknown	
5002	rfe	radio free ethernet	unknown	
5003	fmpro-internal	FileMaker, Inc. - Proprietary transport	unknown	
5985	unknown	unknown	http	
6600	unknown	unknown	unknown	
7788	unknown	unknown	unknown	
8014	unknown	unknown	proxy http over ssl	
8015	unknown	unknown	http over ssl	
8016	unknown	unknown	http over ssl	

8029	unknown	unknown	http over ssl
8568	unknown	unknown	RMIRegistry
8958	unknown	unknown	unknown
9680	unknown	unknown	RMIRegistry
15002	unknown	unknown	unknown
15003	unknown	unknown	unknown
47001	unknown	unknown	http
49669	unknown	unknown	msrpc
49670	unknown	unknown	msrpc
49676	unknown	unknown	msrpc
49703	unknown	unknown	msrpc
49707	unknown	unknown	msrpc
49711	unknown	unknown	msrpc
49713	unknown	unknown	msrpc
49720	unknown	unknown	msrpc
49891	unknown	unknown	unknown
50203	unknown	unknown	msrpc
59767	unknown	unknown	unknown

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:09 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HOST2
```

■□□□□ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1082215281 with a standard deviation of 588659465. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5108 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 3 milli seconds
```

1 Apache Tomcat Web Server Running on Target

QID:	86990
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/03/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
Apache Tomcat is running on this target.
QID Detection Logic (Unauthenicated) :
The qid checks HTTP response header to identify the server name and also sends the GET request to non existing page (abc) and match the Tomcat string in response.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Apache Tomcat webserver running on this host on port: 8015
>Apache Tomcat/9.0.37</h3>Apache Tomcat webserver running on this host on port: 8029
```

1 HTTP Methods Returned by OPTIONS Request port 8016/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

1 HTTP Response Method and Header Information Collected port 8016/tcp

QID:	48118
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8016.

```
GET / HTTP/1.0
Host: host2.enterate.com:8016



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=85E950922BB0FAC7435465F4EED9CC8E; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Date: Sat, 20 Feb 2021 05:41:51 GMT
Connection: close
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 8016/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8016 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8016/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubDomains

1 List of Web Directories port 8016/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/css/	web page
/images/	web page
/images/default/	web page
/images/default/window/	web page

1 Default Web Page port 8016/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:8016



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 8016/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:8016



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

1 SSL Server Information Retrieval port 8016/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8016/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8016/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8016/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

■□□□□ 1 SSL/TLS Protocol Properties port 8016/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 8016/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them.

This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8016/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8016/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption

(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02

(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

1 Web Server Supports HTTP Request Pipelining port 8016/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.16.1.12:8016

GET /Q_Evasive/ HTTP/1.1
Host:172.16.1.12:8016



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=EFB0FFAA7FD202CFFE5EEAE207543C8A; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 20 Feb 2021 06:13:30 GMT

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
```

```
</html>

0

HTTP/1.1 404
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html
Content-Length: 122
Date: Sat, 20 Feb 2021 06:13:30 GMT

<html>
 <body >
  <div id="warning" style="width:100%;text-align:center;padding-top:20px;">404</div>
 </body >
</html>
```

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:45:13 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
```

```
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:46:37 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: host2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:45:13 GMT
Connection: close
Content-Length: 315
```

▮□□□□ 1 HTTP Response Method and Header Information Collected port 8015/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 8015.

```
GET / HTTP/1.0
Host: host2.enterate.com:8015



HTTP/1.1 302
Date: Sat, 20 Feb 2021 05:51:47 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

■□□□□ 1 List of Web Directories port 8015/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/management/	brute force
\	brute force

■□□□□ 1 Default Web Page port 8015/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:8015



HTTP/1.1 302
Date: Sat, 20 Feb 2021 05:51:47 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8015/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:8015



HTTP/1.1 302
Date: Sat, 20 Feb 2021 05:57:54 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: https://host2.enterate.com:8015/samlsso?SAMLRequest=nZNBj9owEIXv%2FRWW7yQhbZatRbKioFWRtm0K2R56M84AVhM79UxY9t%
2FXSaDl0CLUY%2ByZ956%2FmUwfjnXFDuBQW5PycRBxBkbZUptdyp%
2BLx9E9f8jeTFHWVSNmLe3NCn62gMRmiODIt82twbYGtwZ30AqeV08pD2tp5A5qMBQi2rCyO21CJatqI9UPzmZETm9agqHZu526l6aEY8rjZPL%
2B%2Fi6542zhvbSR1OfbEzUoQi%2FnpfYWSdxH4yTs0nkXzh6tU9CnTPlWVgicLRcp949aYi4R9QH%2BXCC23g5JGvKGUTweRfEojoooEclEJO%
2BCydv4O2e5s2SVrT5oM1BpnRFWokZhZA0oSIn17NOTiINIbIYiFB%2BLIh%2FlX9YFZ9%2FOdOOOrudtUPQ8r0s1J1%
2Benej3gd3tAvI8IJ4pWwfSKf99gADKHQRd%2FzS8FB5s4kZ89krLRW4rrV7ZrKrsy9yBJE%2BOXAs95FrSde%2FuRJejbV8qmo4Akl8GztZ5p%2F%
2B1lZXeanApH9wvwcS3kgl%2FZz4tJZT98P1SERyJzW3dSKexgw9Hqei%2FXAYTcak8rzzcFWwv5G6exdUyJVQn7Y%2B7dX2xruzWD5R%
2FWeGkwcY6Gsb21zzZcPcvINl54pc%2FcvYL&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=
Lzak8Aj6BdeBKlVW%2FfeiGL5vrYonMNPKeMYzcfeA3pc8tKvX%2F5MQ0AtzV%2FDHsRDuStLDihCZkrYwgxDQFC9Trt%
2FIiJC5Fi28cvCmmQMZQ1fQUyzJZwUfE5280BxOrA1BYnJTDJ5lUNTmqJ0rS0oxKeKeY552Z6o7HcF9K9%2B%2BOipITNz33kQJ%
2ByPM6dEMBh18KPf%2FSqG6ipPRLpokJjK97OV3UCR2G%2FVW7UDgNGNbNXT68GnCMVczwnxfJeqtVU6%2BAU%2Box2myWG1%
2BSDFtO%2F%2F5P3oqm0hfjDJum6bmiVzrTWAzxZkGZk%2FCHvo%2B%2BxkujLBrbaIlQge9k%2FRjV9GxTeDq1w%3D%3D
Content-Length: 0
Set-Cookie: isDBAvailable=checked
Set-Cookie: EDGEJSESSIONID=7AFC3C766C0957065CCFAFE106894930; Path=/management; Secure; HttpOnly
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

1 SSL Server Information Retrieval port 8015/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8015/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 8015/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8015/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	brainpoolp512r1	512	yes	256	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	brainpoolp384r1	384	yes	192	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low
ECDHE	brainpoolp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 8015/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

▮▯▯▯▯ 1 SSL Certificate Transparency Information port 8015/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8015/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8015/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:

(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:

(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8015/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by

Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.16.1.12:8015

GET /Q_Evasive/ HTTP/1.1
Host:172.16.1.12:8015



HTTP/1.1 302
Date: Sat, 20 Feb 2021 06:13:40 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0

HTTP/1.1 404
Date: Sat, 20 Feb 2021 06:13:40 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 682

<!doctype html><html lang="en"><head><title>HTTP Status 404 _E2_80_93 Not Found</title><style type="text/css">body {font-family:Tahoma,Arial,
sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a
{color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 404 _E2_80_93 Not Found</h1><
hr class="line" /><p><b>Type</b> Status Report</p><p><b>Description</b> The origin server did not find a current representation for the target
resource or is not willing to disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.37</h3></body></html>
```

1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 8014.

```
GET / HTTP/1.0
Host: host2.enterate.com:8014



HTTP/1.1 200
Date: Sat, 20 Feb 2021 06:01:52 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Set-Cookie: AGENTJSESSIONID=A809A455ACBBFCCA30EDAE6BD93B3ABA; Path=/; Secure; HttpOnly
Connection: close
```

▮▯▯▯▯ 1 Referrer-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:

- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Referrer-Policy HTTP Header missing on 8014 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8014/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubDomains

■□□□□ 1 HTTP Service Unavailable Replies Received port 8014/tcp

QID:	86383
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2006
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

We have received "503 Service Unavailable" replies in response to our HTTP requests. The server is temporarily unable to service your request due to maintenance downtime or capacity problems.

IMPACT:

The detection of possible Web Server vulnerabilities can be inconsistent as follows.

- Because our scanner could not access to this service,
there are possibility of missing some vulnerabilities which should be detected.

- If the target host is a Windows host, there is a possibility
that some
vulnerabilities for IIS that should be detected were not detected.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 503 Service Unavailable
Date: Sat, 20 Feb 2021 06:02:58 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Content-Length: 299
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>503 Service Unavailable</title>
</head><body>
<h1>Service Unavailable</h1>
<p>The server is temporarily unable to service your
request due to maintenance downtime or capacity
problems. Please try again later.</p>
</body></html>
```

1 List of Web Directories port 8014/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
\	brute force
/css/	web page
/images/	web page
/images/default/	web page
/images/default/window/	web page

■□□□□ 1 Default Web Page port 8014/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

▮▯▯▯▯ 1 Default Web Page (Follow HTTP Redirection) port 8014/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

1 SSL Server Information Retrieval port 8014/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
 CIPHER                              KEY-EXCHANGE           AUTHENTICATION  MAC      ENCRYPTION(KEY-STRENGTH)     GRADE
```

SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮▯▯▯▯ 1 SSL Session Caching Information port 8014/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

▮□□□□ 1 SSL/TLS invalid protocol version tolerance port 8014/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

▮□□□□ 1 SSL/TLS Key Exchange Methods port 8014/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	brainpoolp512r1	512	yes	256	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	brainpoolp384r1	384	yes	192	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low
ECDHE	brainpoolp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 8014/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8014/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8014/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8014/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:

(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT

(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8014/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.16.1.12:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.16.1.12:8014



HTTP/1.1 200
Date: Sat, 20 Feb 2021 06:13:55 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Set-Cookie: AGENTJSESSIONID=E4F551EB67D73F1953945221856FAED5; Path=/; Secure; HttpOnly
Transfer-Encoding: chunked

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>

0

HTTP/1.1 404
Date: Sat, 20 Feb 2021 06:13:55 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html
Content-Length: 122

<html>
 <body >
  <div id="warning" style="width:100%;text-align:center;padding-top:20px;">404</div>
 </body >
</html>
```

1 HTTP Methods Returned by OPTIONS Request port 8029/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

1 HTTP Response Method and Header Information Collected port 8029/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 8029.

```
GET / HTTP/1.0
Host: host2.enterate.com:8029



HTTP/1.1 404
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 682
Date: Sat, 20 Feb 2021 06:07:26 GMT
Connection: keep-alive
Keep-Alive: timeout=20
```

1 List of Web Directories port 8029/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/management/	brute force

1 Default Web Page port 8029/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:8029


<!doctype html><html lang="en"><head><title>HTTP Status 404  Not Found</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;}
h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;}
.line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 404  Not Found</h1><hr class="line" /><p><b>
Type</b> Status Report</p><p><b>Description</b> The origin server did not find a current representation for the target resource or is not willing to
disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.37</h3></body></html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8029/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:8029



<!doctype html><html lang="en"><head><title>HTTP Status 404  Not Found</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 404  Not Found</h1><hr class="line" /><p><b>Type</b> Status Report</p><p><b>Description</b> The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.37</h3></body></html>
```

1 SSL Server Information Retrieval port 8029/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH

DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8029/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8029/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8029/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

1 SSL/TLS Protocol Properties port 8029/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client

OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8029/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8029/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8029/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1

(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13

(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:08:46 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:08:58 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: host2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:08:46 GMT
Connection: close
Content-Length: 315
```

1 Microsoft SQL Server Cluster Presence Check port 1434/udp

QID:	19101
Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/30/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The scanner probed the target Microsoft SQL Server to determine if a cluster is being used. Using SQL clustering is required for redundancy/fail-over purposes. The results of the check are posted below.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

SQL Cluster Not Installed

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.
```

1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.1					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low

ECDHE	secp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.1	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes

SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:

(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:

(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)

(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.16.1.13 (host3.enterate.com, HOST3) Windows 2016

Vulnerabilities (1)

1 SSL/TLS Server supports TLSv1.1 port 3389/tcp over SSL

QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/22/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.
This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

IMPACT:

Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:

Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1_1

If the test is successful, then the target support TLSv1.1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.1 is supported

Potential Vulnerabilities (1)

1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (55)

■■■□□ 3 Content-Security-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Content-Security-Policy HTTP Header missing on port 8014.
GET / HTTP/1.0
Host: host3.enterate.com:8014
```

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 8014/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 8014.
GET / HTTP/1.0
Host: host3.enterate.com:8014
```

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U4110:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0	135			
DCOM OXID Resolver	0.0	135			
DCOM Remote Activation	0.0	135			
DCOM System Activator	0.0	135, 49698			
Microsoft Cluster Server API	2.0	49718			
Microsoft Distributed Transaction Coordinator	1.0	49864			
Microsoft Local Security Architecture	0.0	49699, 49674			
Microsoft LSA DS Access	0.0	49699, 49674			
Microsoft Network Logon	1.0	49699, 49674			
Microsoft Registry	1.0				\PIPE\winreg
Microsoft Scheduler Control Service	1.0	49698			\PIPE\atsvc
Microsoft Security Account Manager	1.0	49699, 49674			\pipe\lsass
Microsoft Service Control Service	2.0	49711			
Microsoft Task Scheduler	1.0	49698			\PIPE\atsvc
MS Wbem Transport IEnumWbemClassObject	0.0	49698			
MS Wbem Transport IWbemLevel1Login	0.0	49698			
MS Wbem Transport IWbemObjectSink	0.0	49698			
MS Wbem Transport IWbemServices	0.0	49698			
WinHttp Auto-Proxy Service	5.1				\PIPE\W32TIME_ALT
(Unknown Service)	1.0	135			
(Unknown Service)	1.0	49699, 49674			
(Unknown Service)	0.0	49698			
(Unknown Service)	0.0	135			
(Unknown Service)	1.0	49698			
(Unknown Service)	2.0	135			
(Unknown Service)	1.0	49698			\PIPE\atsvc
(Unknown Service)	4.0	49698			
(Unknown Service)	2.0	49698			\PIPE\atsvc
(Unknown Service)	1.0	49698			\pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0	49698			\pipe\LSM_API_service, \pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0	49668			
(Unknown Service)	1.0	49668			\PIPE\InitShutdown
(Unknown Service)	0.0	49699, 49674			
(Unknown Service)	0.0	49699, 49674			\pipe\lsass
(Unknown Service)	2.0	49699, 49674			\pipe\lsass
(Unknown Service)	1.0	49699, 49674			\pipe\lsass
(Unknown Service)	1.0				\pipe\LSM_API_service
(Unknown Service)	0.0				\pipe\LSM_API_service

DHCP Client LRPC Endpoint	1.0	49669	\pipe\eventlog
DHCPv6 Client LRPC Endpoint	1.0	49669	\pipe\eventlog
Event log TCPIP	1.0	49669	\pipe\eventlog
RemoteRegistry Perflib Interface	1.0		\PIPE\winreg
DfsDs service	1.0		\PIPE\wkssvc
Remote Fw APIs	1.0	49701	

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 135, the host's uptime is 3 days, 9 hours, and 11 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1
```

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1
```

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.1.13	host3.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2178,2180-2512,2514-2701,
2703-3342,3344-3388,3390-5630,5632-5984,5986-6128,6130-6599,6601-7999,
8001-8013,8015-26999,27001-42423,42425-47000,47002-49667,49670-49673,
49675-49697,49700,49702-49710,49712-49717,49719-49863,49865-65535

■□□□□ 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 2355 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:16:22 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
host3.enterate.com	NTLM DNS
host3.enterate.com	FQDN
HOST3	NTLM NetBIOS

■□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.

Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:01:18
TCP	443	0:03:50
TCP	2179	0:00:45
TCP	3343	0:07:11
TCP	3389	0:00:59
TCP	5985	0:27:01
TCP	6600	0:02:42
TCP	8000	0:01:54
TCP	8014	0:50:34
TCP	27000	0:02:17
TCP	47001	0:27:05
TCP	49668	0:05:05
TCP	49669	0:05:05
TCP	49674	0:05:26
TCP	49698	0:05:05
TCP	49699	0:05:13
TCP	49701	0:05:21
TCP	49711	0:05:05
TCP	49718	0:05:05
TCP	49864	0:05:29

1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Microsoft Server Message Block (SMBv3) Compression Disabled

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
443	https	http protocol over TLS/SSL	unknown	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
2179	vmrdp	Microsoft RDP for virtual machines	VMRDP	
3343	ms-cluster-net	MS Cluster Net	unknown	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
6600	unknown	unknown	unknown	
8000	irdmi	iRDMI	unknown	
8014	unknown	unknown	http over ssl	
27000	unknown	unknown	unknown	
47001	unknown	unknown	http	
49668	unknown	unknown	msrpc	
49669	unknown	unknown	msrpc	
49674	unknown	unknown	msrpc	
49698	unknown	unknown	msrpc	
49699	unknown	unknown	msrpc	
49701	unknown	unknown	msrpc	
49711	unknown	unknown	msrpc	
49718	unknown	unknown	msrpc	
49864	unknown	unknown	msrpc	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:09 GMT

■□□□□ 1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HOST3

■□□□□ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1020535418 with a standard deviation of 723218441. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5204 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 8 milli seconds
```

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host3.enterate.com:47001


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:45:59 GMT
Connection: close
Content-Length: 315
```

```
        <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host3.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:45:59 GMT
Connection: close
Content-Length: 315

        <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: host3.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:45:59 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 8014/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 8014.

GET / HTTP/1.0
Host: host3.enterate.com:8014


HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
```

```
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=148EC6E831B8A01BC58AEEA909E42CB7; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Date: Sat, 20 Feb 2021 05:54:20 GMT
Connection: close
```

1 Referrer-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8014 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 8014/tcp

QID:	86137
Category:	Web server
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubDomains

■□□□□ 1 List of Web Directories port 8014/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/css/	web page
/images/	web page

/images/default/	web page
/images/default/window/	web page

■□□□□ 1 Default Web Page port 8014/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host3.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
```

```
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8014/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host3.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

1 SSL Server Information Retrieval port 8014/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH

ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8014/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8014/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8014/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low

ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

■□□□□ 1 SSL/TLS Protocol Properties port 8014/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 8014/tcp over SSL

QID:	38718

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8014/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8014/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption

(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:

(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

1 Web Server Supports HTTP Request Pipelining port 8014/tcp over SSL

QID: 86565

Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.16.1.13:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.16.1.13:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=831BA2F93DE2D1D1E745E2FDB3BB6712; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 20 Feb 2021 06:14:18 GMT

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>

0

HTTP/1.1 404
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 0
Date: Sat, 20 Feb 2021 06:14:18 GMT
```

▮▯▯▯▯ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host3.enterate.com:5985
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:54 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host3.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:59 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: host3.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:54 GMT
Connection: close
Content-Length: 315
```

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID: 38704
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.1					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID: 38706
Category: General remote services
CVE ID: -

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.1	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:

(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:

(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.16.1.14 (host4.enterate.com, HOST4) Windows 2016

Vulnerabilities (1)

🟥□□□□ 1 SSL/TLS Server supports TLSv1.1 port 3389/tcp over SSL

QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/22/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.
This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

IMPACT:

Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:

Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1_1

If the test is successful, then the target support TLSv1.1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.1 is supported

Potential Vulnerabilities (1)

🟨□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (55)

■■■□□ 3 Content-Security-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Content-Security-Policy HTTP Header missing on port 8014.
GET / HTTP/1.0
Host: host4.enterate.com:8014
```

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 8014/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 8014.
GET / HTTP/1.0
Host: host4.enterate.com:8014
```

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U4110:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0	135			
DCOM OXID Resolver	0.0	135			
DCOM Remote Activation	0.0	135			
DCOM System Activator	0.0	135, 49702			
Microsoft Cluster Server API	2.0	49722			
Microsoft Distributed Transaction Coordinator	1.0	49866			
Microsoft Local Security Architecture	0.0	49704, 49674			
Microsoft LSA DS Access	0.0	49704, 49674			
Microsoft Network Logon	1.0	49704, 49674			
Microsoft Registry	1.0				\PIPE\winreg
Microsoft Scheduler Control Service	1.0	49702			\PIPE\atsvc
Microsoft Security Account Manager	1.0	49704, 49674			\pipe\lsass
Microsoft Service Control Service	2.0	49703			
Microsoft Task Scheduler	1.0	49702			\PIPE\atsvc
MS Wbem Transport IEnumWbemClassObject	0.0	49702			
MS Wbem Transport IWbemLevel1Login	0.0	49702			
MS Wbem Transport IWbemObjectSink	0.0	49702			
MS Wbem Transport IWbemServices	0.0	49702			
WinHttp Auto-Proxy Service	5.1				\PIPE\W32TIME_ALT
(Unknown Service)	1.0	135			
(Unknown Service)	1.0	49704, 49674			
(Unknown Service)	0.0	49702			
(Unknown Service)	0.0	135			
(Unknown Service)	1.0	49702			
(Unknown Service)	2.0	135			
(Unknown Service)	1.0	49668			
(Unknown Service)	1.0	49668			\PIPE\InitShutdown
(Unknown Service)	0.0	49704, 49674			
(Unknown Service)	0.0	49704, 49674			\pipe\lsass
(Unknown Service)	2.0	49704, 49674			\pipe\lsass
(Unknown Service)	1.0	49704, 49674			\pipe\lsass
(Unknown Service)	1.0	49702			\PIPE\atsvc
(Unknown Service)	4.0	49702			
(Unknown Service)	2.0	49702			\PIPE\atsvc
(Unknown Service)	1.0	49702			\pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0	49702, 49669			\pipe\LSM_API_service, \pipe\eventlog, \pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0				\pipe\LSM_API_service

(Unknown Service)	0.0			\pipe\LSM_API_service
(Unknown Service)	1.0	49669		\pipe\eventlog
Event log TCPIP	1.0	49669		\pipe\eventlog
RemoteRegistry Perflib Interface	1.0			\PIPE\winreg
DfsDs service	1.0			\PIPE\wkssvc
Remote Fw APIs	1.0	49705		

■■□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Based on TCP timestamps obtained via port 135, the host's uptime is 3 days, 8 hours, and 10 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.
```

■■□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.1.14	host4.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2178,2180-2512,2514-2701,
2703-3342,3344-3388,3390-5630,5632-5984,5986-6128,6130-6599,6601-8013,
8015-26999,27001-42423,42425-47000,47002-49667,49670-49673,49675-49701,
49706-49721,49723-49865,49867-65535

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 2364 seconds

Start time: Sat, Feb 20 2021, 05:44:30 GMT

End time: Sat, Feb 20 2021, 06:23:54 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
host4.enterate.com	NTLM DNS
host4.enterate.com	FQDN
HOST4	NTLM NetBIOS

■□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.

Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

▮□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:01:18
TCP	443	0:03:50
TCP	2179	0:00:45
TCP	3343	0:07:13
TCP	3389	0:00:58
TCP	5985	0:27:02
TCP	6600	0:02:50
TCP	8014	0:50:26
TCP	27000	0:02:21
TCP	47001	0:27:01
TCP	49668	0:05:05
TCP	49669	0:05:05
TCP	49674	0:05:05
TCP	49702	0:05:05
TCP	49703	0:05:05
TCP	49704	0:05:05
TCP	49705	0:05:05
TCP	49722	0:05:11
TCP	49866	0:05:05

▮□□□□ 1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Microsoft Server Message Block (SMBv3) Compression Disabled

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
443	https	http protocol over TLS/SSL	unknown	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
2179	vmrdp	Microsoft RDP for virtual machines	VMRDP	
3343	ms-cluster-net	MS Cluster Net	unknown	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
6600	unknown	unknown	unknown	
8014	unknown	unknown	http over ssl	
27000	unknown	unknown	unknown	
47001	unknown	unknown	http	
49668	unknown	unknown	msrpc	
49669	unknown	unknown	msrpc	
49674	unknown	unknown	msrpc	
49702	unknown	unknown	msrpc	
49703	unknown	unknown	msrpc	
49704	unknown	unknown	msrpc	
49705	unknown	unknown	msrpc	
49722	unknown	unknown	msrpc	
49866	unknown	unknown	msrpc	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:44:33 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HOST4

■□□□□ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1157707778 with a standard deviation of 588974465. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5164 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 4 milli seconds
```

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host4.enterate.com:5985


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:47:02 GMT
Connection: close
Content-Length: 315
```

```
        <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host4.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:47:02 GMT
Connection: close
Content-Length: 315

        <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: host4.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:47:02 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 8014/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 8014.

GET / HTTP/1.0
Host: host4.enterate.com:8014


HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
```

```
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=6F8A46955FD33B4C8EAE352C245E6B51; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Date: Sat, 20 Feb 2021 05:54:55 GMT
Connection: close
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8014 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8014/tcp

QID:	86137
Category:	Web server
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubDomains

1 List of Web Directories port 8014/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/css/	web page
/images/	web page

/images/default/	web page
/images/default/window/	web page

1 Default Web Page port 8014/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host4.enterate.com:8014



<!doctype html>
<html>
<head>
  <meta http-equiv="content-type" content="text/html; charset=UTF-8">
  <meta http-equiv="x-ua-compatible" content="IE=EDGE">
  <meta name="gwt:property" content="locale=en">
  <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
  <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
  <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
  <link type="text/css" rel="stylesheet" href="css/common.css">
  <link type="text/css" rel="stylesheet" href="index.css">

  <title></title>
  <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
  <div style="display: none;">
    <img src="images/default/window/icon-error.gif"></img>
    <img src="images/default/window/top-bottom.png"></img>
    <img src="images/default/window/left-corners.png"></img>
    <img src="images/default/window/right-corners.png"></img>
    <img src="images/default/window/top-bottom.png"></img>
    <img src="images/default/window/left-corners.png"></img>
    <img src="images/default/window/right-corners.png"></img>
    <img src="images/default/window/left-right.png"></img>
  </div>
  <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
```

```
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8014/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host4.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

1 SSL Server Information Retrieval port 8014/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH

ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8014/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 8014/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8014/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low

ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

1 SSL/TLS Protocol Properties port 8014/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8014/tcp over SSL

QID:	38718

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8014/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8014/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption

(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:

(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

▮□□□□ 1 Web Server Supports HTTP Request Pipelining port 8014/tcp over SSL

QID: 86565

Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.16.1.14:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.16.1.14:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=E7D357FBB4AC7EE5A2337D46B53B0188; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 20 Feb 2021 06:21:50 GMT

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>

0

HTTP/1.1 404
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 0
Date: Sat, 20 Feb 2021 06:21:50 GMT
```

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host4.enterate.com:47001
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:56 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host4.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:56 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: host4.enterate.com:47001


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:56 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.1					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.1	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:

(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:

(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.16.1.80 (util16-2.enterate.com, UTIL16-2) Windows 2012 R2 Standard

Information Gathered (35)

■■□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2012 R2 Standard	CIFS via TCP Port 445	
Windows 2012 R2/8.1	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	TCP/IP Fingerprint	U3414:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

■■□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0	135			
DCOM OXID Resolver	0.0	135			
DCOM Remote Activation	0.0	135			
DCOM System Activator	0.0	135			
Message Queuing - QM2QM V1	1.0	2103, 2107, 2105, 49177			
Message Queuing - QMRT V1	1.0	2103, 2107, 2105, 49177			
Message Queuing - QMRT V2	1.0	2103, 2107, 2105, 49177			
Message Queuing - RemoteRead V1	1.0	2103, 2107, 2105, 49177			
Microsoft Local Security Architecture	0.0	49172, 49155			
Microsoft LSA DS Access	0.0	49172, 49155			
Microsoft Network Logon	1.0	49172, 49155			
Microsoft Scheduler Control Service	1.0	49154			\PIPE\atsvc
Microsoft Security Account Manager	1.0	49172, 49155			\pipe\lsass
Microsoft Server Service	3.0	49154			
Microsoft Service Control Service	2.0	49180			
Microsoft Task Scheduler	1.0	49154			\PIPE\atsvc
MS Wbem Transport IEnumWbemClassObject	0.0	49154			
MS Wbem Transport IWbemObjectSink	0.0	49154			
MS Wbem Transport IWbemServices	0.0	49154			
WinHttp Auto-Proxy Service	5.1				\PIPE\W32TIME_ALT
(Unknown Service)	1.0	135			
(Unknown Service)	1.0	49172, 49155			
(Unknown Service)	0.0	2103, 2107, 2105, 49177, 49154			
(Unknown Service)	0.0	49154			
(Unknown Service)	1.0	2103, 2107, 2105, 49177			
(Unknown Service)	0.0	135			
(Unknown Service)	1.0	49154			

(Unknown Service)	2.0	135	
(Unknown Service)	0.0	49172, 49155	
(Unknown Service)	0.0	49172, 49155	\pipe\lsass
(Unknown Service)	1.0	49152	
(Unknown Service)	1.0	49152	\PIPE\InitShutdown
(Unknown Service)	1.0	49154	\PIPE\srvsvc, \PIPE\atsvc
(Unknown Service)	4.0	49154	
(Unknown Service)	1.0	49154	\PIPE\atsvc
(Unknown Service)	1.0		\pipe\LSM_API_service
Wcm Service	1.0	49153	\pipe\eventlog
DHCP Client LRPC Endpoint	1.0	49153	\pipe\eventlog
DHCPv6 Client LRPC Endpoint	1.0	49153	\pipe\eventlog
NRP server endpoint	1.0	49153	\pipe\eventlog
Event log TCPIP	1.0	49153	\pipe\eventlog
DfsDs service	1.0		\PIPE\wkssvc
Remote Fw APIs	1.0	49182	

■■□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 135, the host's uptime is 7 days, 21 hours, and 35 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

■■□□ 2 Windows Registry Pipe Access Level

QID:	90194

Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.1.80	util16-2.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 443, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-444,446-1705,1707-1800,1802-1999,2001-2102,2104,2106,2108-2146,
2148-2512,2514-2701,2703-3388,3390-5630,5632-5984,5986-6128,6130-42423,
42425-47000,47002-49151,49156-49171,49173-49176,49178-49179,49181,49183-65535

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2382 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:16:21 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
util16-2.enterate.com	NTLM DNS
util16-2.enterate.com	FQDN
UTIL16-2	NTLM NetBIOS

▮▯▯▯▯ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45261 detected on port 445 over TCP.

SMBv1 is enabled.

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.
```

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:01:18
TCP	445	0:00:59
TCP	3389	0:00:52
TCP	5985	0:27:04
TCP	47001	0:27:06
TCP	49152	0:05:05
TCP	49153	0:05:05
TCP	49154	0:05:05
TCP	49155	0:05:05
TCP	49172	0:05:05
TCP	49177	0:05:05
TCP	49180	0:05:05
TCP	49182	0:05:05

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1801	msmq	Microsoft Message Que	Microsoft Message Queue Server	
2103	zephyr-clt	Zephyr serv-hm connection	msrpc	
2105	minipay	MiniPay	msrpc	
2107	unknown	unknown	msrpc	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
47001	unknown	unknown	http	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	
49155	unknown	unknown	msrpc	
49172	unknown	unknown	msrpc	
49177	unknown	unknown	msrpc	
49180	unknown	unknown	msrpc	
49182	unknown	unknown	msrpc	

■□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:36:40 GMT

■□□□□ 1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

UTIL16-2

■□□□□ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045

Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1135724853 with a standard deviation of 603089974. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5095 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2
Duration: 9 milli seconds
```

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util16-2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:39:37 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util16-2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:39:37 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: util16-2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:39:37 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util16-2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:15 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util16-2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
```

```
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:15 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: util16-2.enterate.com:5985


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:15 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			

Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95

(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)

(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:

(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.16.1.253 (sfr16-2.enterate.com, -)

Information Gathered (5)

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.1.253	sfr16-2.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,
2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,
5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,
7008-7009,7011-8304,8306-9098,9100-9989,9991-10109,10111-42423,42425-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2483 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:18:30 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
sfr16-2.enterate.com	FQDN

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

172.16.1.254 (asa16-2.enterate.com, -)

Information Gathered (5)

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.1.254	asa16-2.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
4,12,14,16,26,28,36,40,44,222,225-228,232,235-236,238-240,247-248,251,
254,266,273,275-278,284-286,288-289,295,297,301-302,306,308,310,314,316,
319,328,330,332,335,338-339,341,343,354-355,360,362,364-366,379,482,509,
550,584,586,589-590,595-597,599,603-605,621,623,632,639,642,645,647,649,
652-653,655-656,660-663,669,676-679,686,689,691-692,694,696-699,701-703,
706,708,721,723,727-728,732-733,736-737,739,745-746,756-757,768,778-779,
785,788,790-792,794,798,802-805,807,809,811,814,816-817,820-821,823,825,
827-828,830-839,841-842,844-847,852,856-859,861-862,864-865,868-869,871,
874,876-878,880,882-885,891-892,894-898,902,904,913-914,921-922,925, and more.
We have omitted from this list 31832 higher ports to keep the report size manageable.
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 443 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 05:44:30 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
asa16-2.enterate.com	FQDN

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)

Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=4)	Fragmented IP Packet	Fragmentation Needed

172.16.10.5 (dc1.enterate.com, DC1) Windows 2016

Potential Vulnerabilities (1)

■■□□□ 2 DNS Server Allows Remote Clients to Snoop the DNS Cache port 53/udp

QID:	15035
Category:	DNS and BIND
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/13/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The DNS server was found to allow DNS cache snooping. This means, any attacker could remotely check if a given domain name is cached on the DNS server.
This issue occurs when a target DNS server allows an untrusted client to make non-recursive DNS queries for domains that the target DNS server is not authoritative on. If the target DNS server consults its cache and replies with a valid answer (the IP address or "does not exist" NXDOMAIN reply), it is vulnerable to this attack. This tells the attacker that someone from the target network recently resolved that particular domain name.
QID Detection Logic (unauthenticated):
We make a DNS A query for testdeadenddummy.qualys.com from the target DNS server. The Recursive Query flag is set in this query. This means that the target DNS server will recursively search for the address of testdeadenddummy.qualys.com domain name and reply with an IP address to our scanner. If we do not get a reply we quit without posting a vuln.
- Next, we make the same DNS "A" query for the same domain-name name testdeadenddummy.qualys.com. However, this time we leave the "Recursive Query" flag unset. This means, we are requesting the target DNS server to check its cache or pre-defined DNS zone information for the IP address of the testdeadenddummy.qualys.com domain name. (If no information is present there, it should not find this information recursively from other DNS servers, and should simply reply with a non-found message). Since no other DNS server will have a zone for qualys.com, if we do get a reply, it has to be from the cache. If we do not get a response, we quit.
- If we do get a valid IP address in the reply, it means the DNS server consulted its cache and replied with the IP address of a site it recently cached. So an attacker can see what sites are cached in the DNS server by making non-recursive "A" requests for them.

IMPACT:

DNS caches are short lived and are generated by a recent DNS name-resolution event. By repeatedly monitoring DNS cache entries over a period of time, an attacker could gain a variety of information about the target network. For example, one could analyze Web-browsing habits of the users of a network. By querying for DNS MX record caches, one could check for email communication between two companies.
Information gathered from the DNS cache could lead to a variety of consequences ranging from an invasion of privacy to corporate espionage. The above mentioned paper presents a couple of attack scenarios where this vulnerability can be used.

SOLUTION:

Here is a suggested solution for the Microsoft Windows DNS server. One rigorous solution involves what is known popularly as a "split DNS" configuration.

The idea is to have two separate DNS servers, one for the DMZ/perimeter of the network that faces the public Internet, while the other is internal and not publically accessible.
The external one has zone information about only the hosts in the DMZ region which need to be accessed from the Internet. It has no information about the internal hosts with non-routable addresses.
The internal one has all the authoritative information about the internal hosts, and also static entries for the services in the DMZ region (so internal users can access those if required).
Typically, the internal DNS server will be Active Directory integrated, with (secure) dynamic updates enabled.
The external DNS server will typically be a standalone (not integrated with the Active Directory) server without any dynamic DNS updates enabled.
To prevent the unrelated DNS cache-poisoning vulnerability, also configure the registry as explained in Microsoft Knowledge Base Article 241352 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;241352) on both the DNS servers.
Both the DNS servers can be named with identical domain names, such as example.com without any conflicts.
The external DNS server should be set as a "forwarder" in the DNS settings of the internal DNS server. This means, for any DNS query (A/PTR) that the internal DNS server receives, that it is not able to resolve, it forwards it to the external DNS server for resolution.
Through the "DNS" MMC snap-in, Recursion should be enabled on the external DNS server, and disabled in the internal one. This prevents the internal DNS server from attempting to resolve DNS queries if the external one fails to do so.
To reinforce the last configuration, the internal DNS server should be set as a "slave" DNS server through the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" key's "IsSlave" value set to 1.
Finally, to prevent cache snooping on the external DNS server, create a "MaxCacheTtl" DWORD entry with value set to 1 under the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" key of the external DNS
server. This makes the TTL of any cached DNS entry on the external DNS server equal to 1 second,
effectively disabling caching on it. Since for any query originating from the internal network,
both the DNS servers cache the responses, performance is not affected at all even by disabling
the external cache - repeated future DNS queries will be picked up by the internal DNS server
and replied to from its cache.

This separates the external DNS proxy from the internal DNS cache, and prevents any DNS cache snooping from the public Internet.

For BIND and the understanding of the issue this URL will be helpful. http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf (http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Server's cache timeout for IPv4 addresses is more than 3 sec.
Server's cache timeout for IPv6 addresses is more than 3 sec.

Information Gathered (78)

■■■□□ 3 Content-Security-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Content-Security-Policy HTTP Header missing on port 8014.
GET / HTTP/1.0
Host: dc1.enterate.com:8014
```

3 HTTP Public-Key-Pins Security Header Not Detected port 8014/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 8014.
GET / HTTP/1.0
Host: dc1.enterate.com:8014
```

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:53
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

■■□□□ 2 DNS Hierarchy of Target DNS Server Traced

QID:	45035
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/15/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This probe traces the hierarchy of the target DNS server. It first makes a non-recursive query to one of the root DNS servers (*.root-servers.net). These servers point the scanner to the next level of DNS servers that handle the top-level domains, like ".com", and ".net". Then this lower-level DNS server is queried for the next-level DNS server and so on. This is repeated until a DNS server that is authoritative on the target hosts's FQDN domain (or has a cached DNS "A" record for the target) is found.
The hierarchy information is presented in the Result section below.
This information can be used to better map the chain of DNS servers from the root servers down to the actual target DNS server. This gives the flow of DNS information through the chain, and also it can help predict which DNS servers are authoritative on which domains.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Level 1: DNS server: B.ROOT-SERVERS.NET. (199.9.14.201)
Level 2: DNS server: b.gtld-servers.net. (192.33.14.30)
Level 3: DNS server: ns10.domaincontrol.com. (173.201.72.5)
Level 4: ns10.domaincontrol.com. knows nothing about dc1.enterate.com.
```

■■□□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0			593	
DCOM OXID Resolver	0.0			593	
DCOM Remote Activation	0.0			593	
DCOM System Activator	0.0	49672		593	

Domain Name System	5.0	52205		
Microsoft Local Security Architecture	0.0	49669, 49666	49670	\pipe\c5611434a3cef28e, \pipe\lsass
Microsoft LSA DS Access	0.0	49669, 49666	49670	
Microsoft Network Logon	1.0	49669, 49666	49670	\pipe\c5611434a3cef28e, \pipe\lsass
Microsoft NT Directory DRS Interface	4.0	49669, 49666	49670	\pipe\c5611434a3cef28e, \pipe\lsass
Microsoft Scheduler Control Service	1.0	49672		\PIPE\atsvc
Microsoft Security Account Manager	1.0	49669, 49666	49670	\pipe\lsass
Microsoft Service Control Service	2.0	51121		
Microsoft Task Scheduler	1.0	49672		\PIPE\atsvc
MS Wbem Transport IEnumWbemClassObject	0.0	49672		
MS Wbem Transport IWbemLevel1Login	0.0	49672		
MS Wbem Transport IWbemObjectSink	0.0	49672		
MS Wbem Transport IWbemServices	0.0	51526, 49672		
MS Windows DHCP Server (API 1)	1.0	52168		
MS Windows DHCP Server (API 2)	1.0	52168		
WinHttp Auto-Proxy Service	5.1			\PIPE\W32TIME_ALT
(Unknown Service)	1.0		593	
(Unknown Service)	1.0	49669, 49666	49670	
(Unknown Service)	0.0	52168, 51526, 49669, 49672, 49666	49670	
(Unknown Service)	0.0	49672		
(Unknown Service)	0.0		593	
(Unknown Service)	1.0	49672		
(Unknown Service)	2.0		593	
(Unknown Service)	0.0	51526		
(Unknown Service)	1.0	51526		
(Unknown Service)	0.0	51526, 49672		
(Unknown Service)	1.0	49664		
(Unknown Service)	1.0	49664		\PIPE\InitShutdown
(Unknown Service)	0.0	49669, 49666	49670	
(Unknown Service)	1.0	49669, 49672, 49666	49670	\PIPE\atsvc, \pipe\lsass
(Unknown Service)	0.0	49669, 49666	49670	\pipe\c5611434a3cef28e, \pipe\lsass
(Unknown Service)	2.0	49669, 49666	49670	\pipe\c5611434a3cef28e, \pipe\lsass
(Unknown Service)	1.0	49669, 49666	49670	\pipe\c5611434a3cef28e, \pipe\lsass
(Unknown Service)	4.0	49672		
(Unknown Service)	1.0	49672		\PIPE\atsvc
(Unknown Service)	2.0	49672		\PIPE\atsvc
(Unknown Service)	1.0	49672		\pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0			\pipe\LSM_API_service
(Unknown Service)	1.0	49665		\pipe\LSM_API_service, \pipe\eventlog
(Unknown Service)	0.0			\pipe\LSM_API_service
(Unknown Service)	1.0	49665		\pipe\eventlog
Event log TCPIP	1.0	49665		\pipe\eventlog
DHCPv6 Client LRPC Endpoint	1.0			\pipe\eventlog
DHCP Client LRPC Endpoint	1.0			\pipe\eventlog
DfsDs service	1.0			\PIPE\wkssvc
Remote Fw APIs	1.0	49692		

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Based on TCP timestamps obtained via port 53, the host's uptime is 4 days, 2 hours, and 17 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.
```

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1
```

■■□□□ 2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.10.5	dc1.enterate.com

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 80, 111, 443, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-52,54-87,89-134,136-388,390-444,446-463,465-592,594-635,637-1705,1707-1999,
2001-2146,2148-2512,2514-2701,2703-2868,2870-3267,3270-3388,3390-5630,
5632-5984,5986-6128,6130-8013,8015-9388,9390-42423,42425-47000,47002-49663,
49667-49668,49671,49673-49691,49693-51120,51122-51525,51527-52167,52169-52204,
52206-65535

1 LDAP Information Gathering

QID:	45016
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

RootDSE is a standard attribute defined in the LDAP Version 3.0 specification. RootDSE contains information about the directory server, including its capabilities and configuration. The search response will contain a standard set of information, which is defined in the following RFC:
RFC 2251-Lightweight Directory Access Protocol(v3) (http://www.cis.ohio-state.edu/htbin/rfc/rfc2251.html)
The root DSE (DSA-Specific Entry) data can be retrieved from an LDAPv3 server by performing a base-level search with a null BaseDN and filter ObjectClass=*. The root DSE publishes information about the LDAP server, including which LDAP versions it supports, any supported SASL mechanisms, supported controls, and the DN for its subschemaSubentry. In addition to server information, operational attributes may be exposed that allow for extended administration functionality.

IMPACT:

The information gathered can be used to launch further attacks against the system or network hosting the LDAP service.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
currentTime: 20210220054948.0Z
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=enterate,DC=co
 m
dsServiceName: CN=NTDS Settings,CN=DC1,CN=Servers,CN=miami_colo,CN=Sites,CN=
 Configuration,DC=enterate,DC=com
namingContexts: DC=enterate,DC=com
namingContexts: CN=Configuration,DC=enterate,DC=com
namingContexts: CN=Schema,CN=Configuration,DC=enterate,DC=com
namingContexts: DC=ForestDnsZones,DC=enterate,DC=com
namingContexts: DC=DomainDnsZones,DC=enterate,DC=com
defaultNamingContext: DC=enterate,DC=com
schemaNamingContext: CN=Schema,CN=Configuration,DC=enterate,DC=com
configurationNamingContext: CN=Configuration,DC=enterate,DC=com
rootDomainNamingContext: DC=enterate,DC=com
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.840.113556.1.4.801
supportedControl: 1.2.840.113556.1.4.473
supportedControl: 1.2.840.113556.1.4.528
supportedControl: 1.2.840.113556.1.4.417
supportedControl: 1.2.840.113556.1.4.619
```

```
supportedControl: 1.2.840.113556.1.4.841
supportedControl: 1.2.840.113556.1.4.529
supportedControl: 1.2.840.113556.1.4.805
supportedControl: 1.2.840.113556.1.4.521
supportedControl: 1.2.840.113556.1.4.970
supportedControl: 1.2.840.113556.1.4.1338
supportedControl: 1.2.840.113556.1.4.474
supportedControl: 1.2.840.113556.1.4.1339
supportedControl: 1.2.840.113556.1.4.1340
supportedControl: 1.2.840.113556.1.4.1413
supportedControl: 2.16.840.1.113730.3.4.9
supportedControl: 2.16.840.1.113730.3.4.10
supportedControl: 1.2.840.113556.1.4.1504
supportedControl: 1.2.840.113556.1.4.1852
supportedControl: 1.2.840.113556.1.4.802
supportedControl: 1.2.840.113556.1.4.1907
supportedControl: 1.2.840.113556.1.4.1948
supportedControl: 1.2.840.113556.1.4.1974
supportedControl: 1.2.840.113556.1.4.1341
supportedControl: 1.2.840.113556.1.4.2026
supportedControl: 1.2.840.113556.1.4.2064
supportedControl: 1.2.840.113556.1.4.2065
supportedControl: 1.2.840.113556.1.4.2066
supportedControl: 1.2.840.113556.1.4.2090
supportedControl: 1.2.840.113556.1.4.2205
supportedControl: 1.2.840.113556.1.4.2204
supportedControl: 1.2.840.113556.1.4.2206
supportedControl: 1.2.840.113556.1.4.2211
supportedControl: 1.2.840.113556.1.4.2239
supportedControl: 1.2.840.113556.1.4.2255
supportedControl: 1.2.840.113556.1.4.2256
supportedControl: 1.2.840.113556.1.4.2309
supportedLDAPVersion: 3
supportedLDAPVersion: 2
supportedLDAPPolicies: MaxPoolThreads
supportedLDAPPolicies: MaxPercentDirSyncRequests
supportedLDAPPolicies: MaxDatagramRecv
supportedLDAPPolicies: MaxReceiveBuffer
supportedLDAPPolicies: InitRecvTimeout
supportedLDAPPolicies: MaxConnections
supportedLDAPPolicies: MaxConnIdleTime
supportedLDAPPolicies: MaxPageSize
supportedLDAPPolicies: MaxBatchReturnMessages
supportedLDAPPolicies: MaxQueryDuration
supportedLDAPPolicies: MaxDirSyncDuration
supportedLDAPPolicies: MaxTempTableSize
supportedLDAPPolicies: MaxResultSetSize
supportedLDAPPolicies: MinResultSets
supportedLDAPPolicies: MaxResultSetsPerConn
supportedLDAPPolicies: MaxNotificationPerConn
supportedLDAPPolicies: MaxValRange
supportedLDAPPolicies: MaxValRangeTransitive
supportedLDAPPolicies: ThreadMemoryLimit
supportedLDAPPolicies: SystemMemoryLimitPercent
highestCommittedUSN: 6893033
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
dnsHostName: dc1.enterate.com
ldapServiceName: enterate.com:dc1$@ENTERATE.COM
serverName: CN=DC1,CN=Servers,CN=miami_colo,CN=Sites,CN=Configuration,DC=ent
 erate,DC=com
supportedCapabilities: 1.2.840.113556.1.4.800
supportedCapabilities: 1.2.840.113556.1.4.1670
supportedCapabilities: 1.2.840.113556.1.4.1791
supportedCapabilities: 1.2.840.113556.1.4.1935
supportedCapabilities: 1.2.840.113556.1.4.2080
supportedCapabilities: 1.2.840.113556.1.4.2237
isSynchronized: TRUE
isGlobalCatalogReady: TRUE
domainFunctionality: 7
forestFunctionality: 7
domainControllerFunctionality: 7
```

▮▯▯▯▯ 1 Active Directory / Windows Network Enumeration Through DNS Service Locator Records

QID:	45023
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/26/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The DNS server is participating in an Active Directory (Windows Network) domain. The server provides Service Locator Resource Records (SRV RR) to clients requesting them. These SRV RRs contain host names and port numbers for the Windows domain services like Domain Controllers, Global Catalog, Kerberos KDC, Kerberos "passwd" services. These services are required by a domain based on Active Directories, and are used by participating workstations during boot up and authentication.
This module gathers information from these SRV RRs about the Active Directory domain.

IMPACT:

Information gathered may be used to better map the network. Services listed are critical for the Active Directory based network to be available.

SOLUTION:

An effective firewall scheme can be used to shield the DNS server from non-participating or external hosts from querying the DNS server for these records.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
DC LDAP: Host = dc1.enterate.com, Port = 389 (TCP)
DC LDAP: Host = dc2.enterate.com, Port = 389 (TCP)
PDC LDAP: Host = dc1.enterate.com, Port = 389 (TCP)
Global Catalog LDAP: Host = dc2.enterate.com, Port = 3268 (TCP)
Global Catalog LDAP: Host = dc1.enterate.com, Port = 3268 (TCP)
DC Kerberos KDC: Host = dc1.enterate.com, Port = 88 (TCP)
DC Kerberos KDC: Host = dc2.enterate.com, Port = 88 (TCP)
LDAP: Host = dc2.enterate.com, Port = 389 (TCP)
LDAP: Host = dc1.enterate.com, Port = 389 (TCP)
Global Catalog: Host = dc1.enterate.com, Port = 3268 (TCP)
Global Catalog: Host = dc2.enterate.com, Port = 3268 (TCP)
Kerberos KDC: Host = dc2.enterate.com, Port = 88 (TCP)
Kerberos KDC: Host = dc1.enterate.com, Port = 88 (TCP)
Kerberos KDC: Host = dc2.enterate.com, Port = 88 (UDP)
Kerberos KDC: Host = dc1.enterate.com, Port = 88 (UDP)
Kpasswd: Host = dc2.enterate.com, Port = 464 (TCP)
Kpasswd: Host = dc1.enterate.com, Port = 464 (TCP)
Kpasswd: Host = dc2.enterate.com, Port = 464 (UDP)
Kpasswd: Host = dc1.enterate.com, Port = 464 (UDP)
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2395 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:16:34 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
dc1.enterate.com	NTLM DNS
dc1.enterate.com	FQDN
DC1	NTLM NetBIOS

▮▯▯▯▯ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.
```

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	53	0:01:57
TCP	135	0:06:41
TCP	389	0:00:08
TCP	445	0:00:09
TCP	593	0:00:45
TCP	636	0:00:59
TCP	3268	0:00:08
TCP	3269	0:01:00
TCP	3389	0:00:51
TCP	5985	0:29:27
TCP	8014	0:51:21
TCP	9389	0:01:54
TCP	47001	0:29:55
TCP	49664	0:05:05
TCP	49665	0:05:05
TCP	49666	0:05:05
TCP	49669	0:05:05
TCP	49670	0:00:45
TCP	49672	0:05:05
TCP	49692	0:05:05
TCP	51121	0:05:05
TCP	51526	0:05:05
TCP	52168	0:05:05
TCP	52205	0:05:05
UDP	53	0:00:13
UDP	123	0:01:24
UDP	464	0:00:07

■□□□□ 1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Microsoft Server Message Block (SMBv3) Compression Disabled

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Enabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default
CIFS Version	SMB v1 NT LM 0.12

▮▯▯▯▯ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
53	domain	Domain Name Server	named udp
123	ntp	Network Time Protocol	ntp
464	kpasswd	kpasswd	Kerberos Password

▮▯▯▯▯ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
53	domain	Domain Name Server	DNS Server	
88	kerberos	Kerberos	Kerberos-5	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
389	ldap	Lightweight Directory Access Protocol	ldap	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
464	kpasswd	kpasswd	Kerberos Password	
593	http-rpc-epmap	HTTP RPC Ep Map	msrpc-over-http	
636	ldaps	ldap protocol over TLS/SSL (was sldap)	ldap over ssl	
3268	msft-gc	Microsoft Global Catalog	ldap	
3269	msft-gc-ssl	Microsoft Global Catalog with LDAP/SSL	ldap over ssl	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
8014	unknown	unknown	http over ssl	
9389	unknown	unknown	unknown	
47001	unknown	unknown	http	
49664	unknown	unknown	msrpc	
49665	unknown	unknown	msrpc	
49666	unknown	unknown	msrpc	
49669	unknown	unknown	msrpc	
49670	unknown	unknown	msrpc-over-http	
49672	unknown	unknown	msrpc	
49692	unknown	unknown	msrpc	
51121	unknown	unknown	msrpc	
51526	unknown	unknown	msrpc	
52168	unknown	unknown	msrpc	
52205	unknown	unknown	msrpc	

■□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:36:40 GMT

■□□□□ 1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DC1

■□□□□ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045

Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1014089839 with a standard deviation of 667800990. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5101 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 53: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 11 milli seconds
```

▮▯▯▯▯ 1 SSL Server Information Retrieval port 3269/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH

ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 3269/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3269/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 3269/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low

ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3269/tcp over SSL

QID: 38706
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3269/tcp over SSL

QID: 38717

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

▮▯▯▯▯ 1 SSL Certificate Transparency Information port 3269/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3269/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3269/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:

(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:

(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:04 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

▮▯▯▯▯ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:05 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: dc1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:04 GMT
Connection: close
Content-Length: 315
```

1 SSL Server Information Retrieval port 636/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH

AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 636/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 636/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016

User Modified: -
Edited: No
PCI Vuln: No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 636/tcp over SSL

QID: 38704
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

■□□□□ 1 SSL/TLS Protocol Properties port 636/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server

OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 636/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

■□□□□ 1 SSL Certificate Transparency Information port 636/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 636/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 Microsoft Windows Active Directory / Domain Controller Present port 636/tcp over SSL

QID:	45022
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Active Directory is present on the remote system. The system is running as a Domain Controller.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 SSL Certificate - Information port 636/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/

(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36

(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	

(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 8014/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8014.

```
GET / HTTP/1.0
Host: dc1.enterate.com:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=9A4F3A2762E31250B2AB90165734D3CD; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Date: Sat, 20 Feb 2021 05:55:56 GMT
Connection: close
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8014 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8014/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubDomains

1 List of Web Directories port 8014/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/css/	web page
/images/	web page
/images/default/	web page
/images/default/window/	web page

1 Default Web Page port 8014/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc1.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 8014/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc1.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

▮□□□□ 1 SSL Server Information Retrieval port 8014/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8014/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8014/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8014/tcp over SSL

QID: 38704
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

1 SSL/TLS Protocol Properties port 8014/tcp over SSL

QID: 38706
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018

User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 8014/tcp over SSL

QID: 38718
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 08/22/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

▮▯▯▯▯ 1 TLS Secure Renegotiation Extension Support Information port 8014/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

▮▯▯▯▯ 1 SSL Certificate - Information port 8014/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT

(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:

(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

1 Web Server Supports HTTP Request Pipelining port 8014/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which

is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.16.10.5:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.16.10.5:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=6016B9982F57070E0A0A3CF32563F818; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 20 Feb 2021 06:14:34 GMT

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
```

```
</body>
</html>

0

HTTP/1.1 404
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 0
Date: Sat, 20 Feb 2021 06:14:34 GMT
```

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:58:25 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:58:48 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: dc1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:58:25 GMT
Connection: close
Content-Length: 315
```

1 Microsoft Windows Active Directory / Domain Controller Present port 389/tcp

QID:	45022
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Active Directory is present on the remote system. The system is running as a Domain Controller.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮▯▯▯▯ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

▮▯▯▯▯ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:

(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:

(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.16.10.22 (db1.enterate.com, DB1) Windows 2016/2019/10

Potential Vulnerabilities (4)

🟨🟨🟨🟨□ 4 Multiple MS-SQL-7 threats - (I)

QID:	19058
Category:	Database
CVE ID:	CVE-2000-1081, CVE-2001-0542, CVE-2002-0056, CVE-2002-0154
Vendor Reference:	-
Bugtraq ID:	2030, 3733, 4135
Service Modified:	11/13/2019

User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

We can remotely detect the presence of Microsoft's SQL Server, but cannot remotely detect if a patch or service pack has already been applied. Verify that you have applied the appropriate patch and/or service pack.
Note: This would appear as a potential for MSSQL versions 9 and above for an unauthenticated scan. MSSQL versions 9 and above are not vulnerable for these issues.
The following threats are present in MS-SQL-7:
1) Microsoft SQL Server/Data Engine various xp_ Buffer Overflow Vulnerabilities. The API Srv_paraminfo() function is implemented by Extended Stored Procedures (XPs). XPs are DLL files that perform high-level functions. When called, they invoke a function called Srv_paraminfo(), which parses the input parameters. Srv_paraminfo() does not check the length of the parameter string that an XP passes to it. The following XPs are affected: xp_displayparamstmt, xp_enumresultset, xp_showcolv, xp_updatecolvbm, xp_peekqueue, xp_printstatements, xp_proxiedmetadata and xp_SetSQLSecurity.
2) Microsoft SQL Server Multiple Overflow and Format String Vulnerabilities
. SQL Server provides built-in functions for the formatting of error messages based on C-style format specifiers. These built-in functions are accessible to all users. Providing maliciously crafted input to these functions results in exploitable error conditions in the SQL Server process. To mount this attack, the malicious user must have permission to execute SQL queries either directly or by leveraging SQL Command Injection flaws.
3) Microsoft SQL Server Provider Name Buffer Overflow Vulnerability
. SQL Server does not perform proper bounds checking of the provider arguments to the OpenDataSource and OpenRowset functions. These functions may be used by an ordinary user to reference OLE DB data sources. As a result, it is possible to cause a buffer overflow condition to occur by providing an excessively long string as a provider name in a query.
4) Microsoft SQL Server xp_dirtree Buffer Overflow Vulnerability
. A vulnerability has been reported in the xp_dirtree function. If an extremely large parameter is passed to the stored procedure xp_dirtree, a buffer overflow condition will occur. This issue may be related to an older known problem with unsafe usage of the Srv_paraminfo() function call.
5) Microsoft SQL Server Administrator Cached Connection Vulnerability
. Query methods are SQL Server commands used to request information from the database. A flaw exists in the handling of specially structured ad hoc queries, which could enable a normal user to gain administrative privileges. In order to gain access to information in the database, a user must make a connection to the server. Once access to the database is no longer required, the user logging off will terminate the connection. However, by design, SQL Server will store the connection used by the user in cache for a certain amount of time. This is done to improve the server's performance. Next time that particular user logs in, SQL Server can reinstate the cached connection rather than creating a new one.
6) Microsoft SQL Server 7.0 NULL Data DoS Vulnerability. SQL Server will crash if it receives a TDS header with three or more NULL bytes as data. The crash will generate an event in the log with ID 17055 "fatal exception EXCEPTION_ACCESS VIOLATION".
7) Microsoft SQL Server 7.0 Stored Procedure Vulnerability. It is possible for users without the proper permissions to run stored procedure code. This includes a full range of tasks, such as modifying, viewing, or deleting entries in the database. This can be accomplished by executing a stored procedure owned by the SA account, which is referenced from a temporary stored procedure. SQL Server does not properly check the execute permissions on stored procedures referenced by temporary stored procedures.

IMPACT:

1) This vulnerability can only be exploited by users who can successfully log on to the SQL server. By exploiting this vulnerability, it may be possible for malicious users to execute arbitrary code on the host running a vulnerable version of SQL Server. The malicious user would need to overwrite the return address of the calling function with the address of attacker-supplied shell code in memory. This shell code would be executed under the context of the account that the SQL Server service was configured to run under. The account must have a minimum of SYSTEM privileges.
2) By exploiting this vulnerability, it may be possible for malicious users to execute arbitrary code on a host running a vulnerable version of Microsoft's SQL Server.
3) Successful exploitation of this vulnerability could allow a malicious user to execute arbitrary code with the privileges of the database. There is a possibility that this issue may be exploited remotely, either via distributed SQL queries or potentially via an SQL injection attack.
4) If an extremely large parameter is passed to a vulnerable stored procedure, a buffer overflow condition will occur. Depending on the data supplied, this may cause a denial of service condition, or result in the execution of arbitrary code as the SQL Server process.
5) By exploiting this vulnerability, logged-in users can gain administrative privileges to the database.
6) If this vulnerability is exploited, the SQL server will crash.
7) Users must be authenticated on the SQL server and have access to the referring database in order to perform this exploit. By exploiting this vulnerability, it's possible for users without the proper permissions to run database stored procedure code.

SOLUTION:

1) Read Microsoft Security Bulletin MS00-092: Frequently Asked Questions (http://www.microsoft.com/technet/security/bulletin/MS00-092.mspx) for more information about this vulnerability and for instructions on how to download and install the patches.
2) Read Microsoft Security Bulletin MS01-060 (http://www.microsoft.com/technet/security/bulletin/MS01-060.mspx) for more information about this vulnerability and for instructions on how to download and install the patches.
3,4,5,6,7) Update to Microsoft SQL 7.0 SP4 (http://support.microsoft.com/kb/889543) or higher to resolve theses issues.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
889543: MS SQL 7 (http://support.microsoft.com/kb/889543)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2000-1081
Description:	Microsoft SQL Server 7.0/2000 / Data Engine 1.0/2000 - xp_displayparamstmt Buffer Overflow - The Exploit-DB Ref : 20451
Link:	http://www.exploit-db.com/exploits/20451

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

■■■■□ 4 Multiple MS-SQL-7 threats - (II)

QID:	19059
Category:	Database
CVE ID:	CVE-2000-0202, CVE-2002-0643, CVE-2002-0721
Vendor Reference:	-
Bugtraq ID:	5203, 1041
Service Modified:	11/13/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
We can remotely detect the presence of Microsoft's SQL Server, but cannot remotely detect if a patch or service pack has already been applied. Verify that you have applied the appropriate patch and/or service pack.
The following threats are present in MS-SQL-7:
1) Microsoft SQL Server Non-Validated Query Vulnerability. SQL Server 7.0 and Data Engine (SQL-compatible add-on for Access 2000 and Visual Studio 6.0) will accept SQL queries that can lead to a compromise of the database or the underlying operating system. It's possible for any SQL-authenticated user to pass commands through SQL SELECT statements, which will be run at the privilege level of the database owner or administrator.
2) Microsoft SQL Server Installation Password Caching Vulnerability. During the initial installation of Microsoft SQL Server 7 (including MSDE 1.0) or the installation of service packs, information is gathered and stored in a special file that can later be used to automate other MS-SQL Server installations. This file, setup.iss, may contain passwords supplied during the installation process. In addition, the log file documenting the installation process will also contain any passwords entered. The passwords are first encrypted and then stored. The Microsoft released bulletin notes that the encryption may potentially be weak. During the installation process, passwords may be stored in either of the following two cases:

If the SQL Server is being set up in "Mixed Mode", a password for the SQL Server administrator (the ?sa? account) must be supplied.
Whether in Mixed Mode or Windows Authentication Mode, a User ID and password can optionally be supplied for the purpose of starting up SQL Server service accounts.
Contributing to the vulnerability (in versions of SQL Server 7.0), this file is stored on the server in a location that can be viewed by anyone with rights to log on interactively.
3) Microsoft SQL Agent Jobs Privilege Elevation Vulnerability. SQL Server uses an Agent, which is responsible for restarting the SQL Server service, replication, and running scheduled jobs. Some of the jobs supplied by Microsoft as stored procedures on the SQL Server contain weak permissions. The following procedures are affected:
sp_add_job, sp_add_jobstep, sp_add_jobserver, and sp_start_job.
The Agent typically runs in the security context of the SQL Server Service Account. Under normal circumstances, when a T-SQL job is submitted to the Agent, it will drop its privilege level by performing the following command: SETUSER N'guest' WITH NORESET
4) Microsoft SQL Server Extended Stored Procedure Privilege Elevation Vulnerability. Some of the extended stored procedures supplied by Microsoft contain weak permissions. The extended stored procedures typically connect to the database in the security context of the SQL Server Service Account. Users with low privileges could pass certain arguments to the vulnerable extended stored procedures, allowing them to perform actions on the database in the security context of the SQL Server Service Account. The vulnerability could also be exploited by an attacker visiting a Web site that uses one of these extended stored procedures as part of a search engine for the database. The database-driven Web application would need to be prone to existing input validation vulnerabilities for this type of exploitation to occur.
Note: This would appear as a potential for MSSQL versions 8, 9 and above for an unauthenticated scan. MSSQL versions 8,9 and above are not vulnerable for these issues.

IMPACT:
1) The successful exploitation of this vulnerability could lead to a compromise of the database or underlying operating system.
2) If exploited by a malicious user, passwords stored in setup.iss, which are supplied during the installation process, may be stolen.
3) By exploiting this vulnerability, a malicious user would be able to execute other extended stored procedures, such as xp_cmdshell, on the SQL Server with the security context of the SQL Server Service Account.
4) If this vulnerability is exploited, a user with low privileges may perform actions on the database in the security context of the SQL Server Service Account.

SOLUTION:

1) This can be bypassed by causing the Agent to reconnect after it has performed the privilege lowering command. A malicious user can achieve this using the extended stored procedures discussed in the Microsoft SQL Server Extended Stored Procedure Privilege Elevation Vulnerability (BID 5481). It is not currently clear if this issue was addressed in Microsoft Security Bulletin MS02-043 (http://www.microsoft.com/technet/security/bulletin/MS02-043.mspx). However, applying the patch for that issue will significantly mitigate potential exploitation of this vulnerability by preventing attackers from using the vulnerable extended stored procedures to cause the SQL Server Agent to reconnect to the database with a higher privilege level. The bulletin includes instructions for obtaining the patch. Check for upgrades at Microsoft's Download site (http://www.microsoft.com/sql/downloads/default.asp).
2) Microsoft released the following fix for SQL server 7.0: Patch Q327068 (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q327068&sd=tech)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
889543: MS SQL 7 (http://support.microsoft.com/kb/889543)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2002-0721
Description:	Microsoft SQL 2000/7.0 - Agent Jobs Privilege Escalation - The Exploit-DB Ref : 21718
Link:	http://www.exploit-db.com/exploits/21718

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

🟨🟨🟨□□ 3 SMB Signing Disabled or SMB Signing Not Required

QID:	90043
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/08/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This host does not seem to be using SMB (Server Message Block) signing. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol.
SMB signing adds security to a network using NetBIOS, avoiding man-in-the-middle attacks.
When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.
QID Detection Logic:
This checks from the registry value of RequireSecuritySignature and EnableSecuritySignature form HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkStation\Parameters for client and HKEY_LOCAL_MACHINE\System\CurrentControlSetServices\LanmanServer\Parameters for servers to check if SMB signing is required or enabled or disabled.
Note: On 5/28/2020 the QID was updated to check for client SMB signing behavior via the registry key HKEY_LOCAL_MACHINE\SystemCurrent\ControlSetServices\LanmanWorkStation\Parameters. The complete detection logic is explained above.

IMPACT:

Unauthorized users sniffing the network could catch many challenge/response exchanges and replay the whole thing to grab particular session keys, and then authenticate on the Domain Controller.

SOLUTION:

Without SMB signing, a device could intercept SMB network packets from an originating computer, alter their contents, and broadcast them to the destination computer. Since, digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity, it is recommended that SMB signing is enabled and required.
Please refer to Microsoft's article 887429 (http://support.microsoft.com/kb/887429) and The Basics of SMB Signing (covering both SMB1 and SMB2) (https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2) for information on enabling SMB signing.
For Windows Server 2008 R2, Windows Server 2012, please refer to Microsoft's article Require SMB Security Signatures (http://technet.microsoft.com/en-us/library/cc731957.aspx) for information on enabling SMB signing. For group policies please refer to Microsoft's article Modify Security

Policies in Default Domain Controllers Policy (http://technet.microsoft.com/en-us/library/cc731654)
For UNIX systems
To require samba clients running "smbclient" to use packet signing, add the following to the "[global]" section of the Samba configuration file:
client signing = mandatory

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

2 Database Instance Detected port 9822/tcp

QID:	19568
Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The service detected a database installation on the target. Databases like Oracle, MS-SQL, MySQL, IBM DB2, PostGgresql, Firebird and other are detected. The database instance is listed in the result section below.

IMPACT:
Information disclosing database type will lead attacker to perform more targeted attacks.

SOLUTION:
Users are recommended to encrypt the database information and handle the situations where any error is leading to disclose some sensitive information like database type and its version.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
POSTGRESQL instance detected on TCP port 9822.

Information Gathered (49)

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016/2019/10	NTLMSSP	
Windows Server 2019 Standard 17763/Windows Server 2019 Standard 6.3	CIFS via TCP Port 445	

■■□□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Message Queuing - QM2QM V1	1.0	2103, 2107, 49702, 2105			
Message Queuing - QMRT V1	1.0	2103, 2107, 49702, 2105			
Message Queuing - QMRT V2	1.0	2103, 2107, 49702, 2105			
Message Queuing - RemoteRead V1	1.0	2103, 2107, 49702, 2105			
Microsoft Local Security Architecture	0.0	49666, 49668			
Microsoft LSA DS Access	0.0	49666, 49668			
Microsoft Network Logon	1.0	49666, 49668			
Microsoft Security Account Manager	1.0	49666, 49668			
(Unknown Service)	1.0	49666, 49668			
(Unknown Service)	0.0	2103, 2107, 49702, 2105			
(Unknown Service)	1.0	2103, 2107, 49702, 2105			
(Unknown Service)	0.0	49666, 49668			
(Unknown Service)	2.0	49666, 49668			
(Unknown Service)	1.0	49664			

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Access to Remote Registry Service is denied, error: 0x0

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.10.22	db1.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 443, 1.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-138,140-381,383-444,446-1432,1434-1800,1802-2102,2104,2106,
2108-2868,2870-3388,3390-5984,5986-6128,6130-9821,9823-47000,47002-49663,
49667,49669-49688,49690-49694,49696-49700,49703-49707,49709-49730,49732-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 2450 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:17:29 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
db1.enterate.com	NTLM DNS
db1.enterate.com	FQDN
DB1	NTLM NetBIOS

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:07:55
TCP	139	0:01:09
TCP	445	0:00:09
TCP	1433	0:01:28
TCP	3389	0:00:50
TCP	5985	0:28:13
TCP	9822	0:03:03
TCP	47001	0:32:43
TCP	49664	0:05:05
TCP	49665	0:05:05
TCP	49666	0:05:05
TCP	49668	0:05:05
TCP	49689	0:05:05
TCP	49695	0:05:05
TCP	49701	0:05:05
TCP	49702	0:05:05
TCP	49708	0:05:05
TCP	49731	0:05:05

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	(none)

Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default
CIFS Version	SMB v1 NT LM 0.12

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1433	ms-sql-s	Microsoft-SQL-Server	mssql	
1801	msmq	Microsoft Message Que	Microsoft Message Queue Server	
2103	zephyr-clt	Zephyr serv-hm connection	msrpc	
2105	minipay	MiniPay	msrpc	
2107	unknown	unknown	msrpc	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
9822	unknown	unknown	PostgreSQL	
47001	unknown	unknown	http	
49664	unknown	unknown	msrpc	

49665	unknown	unknown	msrpc
49666	unknown	unknown	msrpc
49668	unknown	unknown	msrpc
49689	unknown	unknown	msrpc
49695	unknown	unknown	msrpc
49701	unknown	unknown	msrpc
49702	unknown	unknown	msrpc
49708	unknown	unknown	msrpc
49731	unknown	unknown	msrpc

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:36:40 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DB1

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 964649452 with a standard deviation of 580068224. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5110 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 15 milli seconds
```

1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: db1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:42:56 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: db1.enterate.com:5985
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:42:57 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: db1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:42:56 GMT
Connection: close
Content-Length: 315
```

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			

Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95

(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)

(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:

(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

1 SSL Server Information Retrieval port 1433/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 1433/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 1433/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 1433/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 1433/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended.

Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

▮□□□□ 1 SSL Certificate OCSP Information port 1433/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 1433/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 1433/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 1433/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1

(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13

(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:

(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: db1.enterate.com:47001


HTTP/1.1 404 Not Found
```

```
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:54:59 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

▮▯▯▯▯ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: db1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:55:00 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: db1.enterate.com:47001


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:54:59 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 9822/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮□□□□ 1 SSL Session Caching Information port 9822/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is disabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 9822/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 9822/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 9822/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 9822/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 9822/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 9822/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:

(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT

(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

172.16.30.15 (util16-1.enterate.com, UTIL16-1) Windows 2016

Information Gathered (65)

▮▮▮▯▯ 3 HTTP Public-Key-Pins Security Header Not Detected rdg.enterate.com:443/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: rdg.enterate.com

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:80
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

■■□□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0			593	
DCOM OXID Resolver	0.0			593	
DCOM Remote Activation	0.0			593	
DCOM System Activator	0.0	64438		593	
Microsoft Local Security Architecture	0.0	49666, 49677			
Microsoft LSA DS Access	0.0	49666, 49677			
Microsoft Network Logon	1.0	49666, 49677			
Microsoft Scheduler Control Service	1.0	64438			\PIPE\atsvc
Microsoft Security Account Manager	1.0	49666, 49677			\pipe\lsass
Microsoft Service Control Service	2.0	64441			
Microsoft Task Scheduler	1.0	64438			\PIPE\atsvc
MS Wbem Transport IEnumWbemClassObject	0.0	64438			
MS Wbem Transport IWbemLevel1Login	0.0	64438			
MS Wbem Transport IWbemObjectSink	0.0	64438			
MS Wbem Transport IWbemServices	0.0	64438			
MSIE IRegExp2	0.0	64438			
(Unknown Service)	1.0			593	
(Unknown Service)	1.0	49666, 49677			
(Unknown Service)	0.0	64438		3388	
(Unknown Service)	0.0	64438			
(Unknown Service)	0.0			593	

(Unknown Service)	1.0	64438		
(Unknown Service)	2.0		593	
DCOM Class Factory	0.0	64438		
(Unknown Service)	1.3		3388	
(Unknown Service)	1.0		3388	
(Unknown Service)	4.0	64438		
(Unknown Service)	1.0	64438		\PIPE\atsvc
(Unknown Service)	2.0	64438		\PIPE\atsvc
(Unknown Service)	1.0	64438		\pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0	64438, 49665		\pipe\LSM_API_service, \pipe\eventlog, \pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	0.0	49666, 49677		
(Unknown Service)	0.0	49666, 49677		\pipe\lsass
(Unknown Service)	2.0	49666, 49677		\pipe\lsass
(Unknown Service)	1.0	49666, 49677		\pipe\lsass
(Unknown Service)	1.0	49664		
(Unknown Service)	1.0	49664		\PIPE\InitShutdown
(Unknown Service)	1.0			\pipe\LSM_API_service
(Unknown Service)	0.0			\pipe\LSM_API_service
(Unknown Service)	1.0	49665		\pipe\eventlog
Event log TCPIP	1.0	49665		\pipe\eventlog
DHCPv6 Client LRPC Endpoint	1.0			\pipe\eventlog
DHCP Client LRPC Endpoint	1.0			\pipe\eventlog
DfsDs service	1.0			\PIPE\wkssvc
(Unknown Service)	1.0	64483		
Remote Fw APIs	1.0	64433		

■■□□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 80, the host's uptime is 4 days, 12 hours, and 49 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe.
Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

2 Web Server HTTP Protocol Versions rdg.enterate.com:80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions rdg.enterate.com:443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions rdg.enterate.com:47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions rdg.enterate.com:5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.30.15	rdg.enterate.com

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 1, 7, 11.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-134,136-442,444,446-592,594-1705,1707-1999,2001-2146,2148-2512,
2514-2701,2703-2868,2870-3387,3390-5630,5632-5984,5986-6128,6130-42423,
42425-47000,47002-49663,49667-49676,49678-55079,55081-64432,64434-64437,
64439-64440,64442-64482,64484-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2379 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:16:18 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
util16-1.enterate.com	NTLM DNS
rdg.enterate.com	FQDN
UTIL16-1	NTLM NetBIOS

■□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.
```

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.
```

1 Scan Activity per Port

QID:	45426

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:36:18
TCP	135	0:07:33
TCP	443	0:42:49
TCP	593	0:00:45
TCP	3388	0:00:45
TCP	3389	0:00:51
TCP	5985	0:27:26
TCP	47001	0:28:45
TCP	49664	0:05:05
TCP	49665	0:05:05
TCP	49666	0:05:05
TCP	49677	0:05:05
TCP	64433	0:05:05
TCP	64438	0:05:05
TCP	64441	0:05:05
TCP	64483	0:05:08

▮□□□□ 1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Microsoft Server Message Block (SMBv3) Compression Disabled

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
593	http-rpc-epmap	HTTP RPC Ep Map	msrpc-over-http	
3388	cbserver	CB Server	msrpc-over-http	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
47001	unknown	unknown	http	
49664	unknown	unknown	msrpc	
49665	unknown	unknown	msrpc	
49666	unknown	unknown	msrpc	
49677	unknown	unknown	msrpc	
64433	unknown	unknown	msrpc	
64438	unknown	unknown	msrpc	
64441	unknown	unknown	msrpc	
64483	unknown	unknown	msrpc	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)

Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:36:40 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
UTIL16-1

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1074709343 with a standard deviation of 650716279. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5207 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 80: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 10 milli seconds
```

■□□□□ 1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 18 Jul 2018 01:38:31 GMT
Accept-Ranges: bytes
ETag: "f19c98381ed41:0"
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:39:18 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
```

```
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 80/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com


HTTP/1.1 200 OK
```

```
Content-Type: text/html
Last-Modified: Wed, 18 Jul 2018 01:38:31 GMT
Accept-Ranges: bytes
ETag: "f19c98381ed41:0"
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:39:45 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 18 Jul 2018 01:38:31 GMT
Accept-Ranges: bytes
ETag: "f19c98381ed41:0"
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:41:43 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 18 Jul 2018 01:38:31 GMT
Accept-Ranges: bytes
ETag: "f19c98381ed41:0"
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:42:31 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
```

```
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM

AES256-SHA256	RSA	RSA	SHA256 AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED				

1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 443/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=rdg.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

■□□□□ 1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=rdg.enterate.com, OU=Domain Control Validated			
Certificate	yes	Google 'Pilot' log	ct.googleapis.com/pilot/	a4b90990b418581487bb13a2cc67700a3c359804f91bdfb8e377cd0ec80ddc10	Mon 18 May 2020 11:15:29 AM GMT
Certificate	yes	Google 'Skydiver' log	ct.googleapis.com/skydiver/	bbd9dfbc1f8a71b593942397aa927b473857950aab52e81a909664368e1ed185	Mon 18 May 2020 11:15:29 AM GMT
Certificate	yes	DigiCert Log Server	ct1.digicert-ct.com/log/	5614069a2fd7c2ecd3f5e1bd44b23ec74676b9bc99115cc0ef949855d689d0dd	Mon 18 May 2020 11:15:30 AM GMT

1 TLS Secure Renegotiation Extension Support Information

port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information

port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	35:3b:be:81:b7:f5:43:0c
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	rdg.enterate.com
(0)Valid From	May 18 11:15:28 2020 GMT
(0)Valid Till	Jul 18 01:15:33 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c7:94:fc:c9:c6:0f:67:a7:16:7d:f2:e2:90:10:
(0)	48:95:98:6c:81:bf:9b:ac:50:cb:e4:08:2d:65:74:
(0)	88:ae:a2:66:f2:5e:c4:04:10:23:4b:ff:c0:aa:d1:
(0)	6b:38:8e:bd:c7:d0:2f:f2:4d:11:0d:99:d4:48:95:
(0)	fe:c0:9a:9e:99:ff:76:32:e4:2f:c3:45:f0:a4:b5:
(0)	e7:1d:f6:cb:a0:af:67:03:4c:6a:bd:aa:22:f1:d1:
(0)	b7:d5:8f:9d:1d:43:62:2d:dc:f3:7d:38:51:b0:b3:
(0)	ea:d8:b8:9a:cd:dc:dc:54:cf:8c:01:e7:38:4b:d1:
(0)	b1:16:ee:16:84:0d:89:7d:64:ba:b0:77:a8:dc:8c:
(0)	88:99:5a:e6:79:bd:a7:fa:bf:9e:4b:27:37:2b:45:

(0)	3b:4d:28:30:c6:a8:83:b3:58:bc:a3:fd:64:02:00:
(0)	3c:10:11:48:e8:af:25:96:43:6b:dd:17:10:dd:73:
(0)	a5:0d:11:d8:58:1a:17:00:cb:13:b7:ab:15:97:7e:
(0)	90:97:eb:38:88:53:aa:f6:c0:85:1e:6c:be:64:74:
(0)	48:ba:78:fe:e2:10:02:19:e6:f4:98:a8:0d:ce:38:
(0)	17:0a:df:53:f7:ad:46:30:78:9a:b2:ab:52:70:e0:
(0)	d8:a6:e6:a1:ed:ad:0c:08:6d:ac:07:71:68:dc:e0:
(0)	6c:f9
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-1972.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:rdg.enterate.com, DNS:www.rdg.enterate.com, DNS:qa-web1.enterate.com, DNS:web1.enterate.com
(0)X509v3 Subject Key Identifier	70:D4:47:52:36:50:C5:11:9B:F6:72:3C:ED:34:62:36:DE:FF:85:AB
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
(0)	3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
(0)	Timestamp : May 18 11:15:29.271 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:D4:2B:E7:DE:66:C3:9E:F5:AF:71:65:
(0)	6F:C0:3D:C3:C3:A4:40:64:E1:9F:8D:61:7D:8B:33:DE:
(0)	58:54:B8:59:54:02:21:00:BB:46:24:BD:59:18:AF:62:
(0)	AA:EC:27:90:34:B5:26:19:0B:45:EF:38:29:88:CF:08:
(0)	27:1D:B8:E4:63:FD:03:15
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : BB:D9:DF:BC:1F:8A:71:B5:93:94:23:97:AA:92:7B:47:
(0)	38:57:95:0A:AB:52:E8:1A:90:96:64:36:8E:1E:D1:85
(0)	Timestamp : May 18 11:15:29.932 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:20:56:EC:A4:48:42:65:69:57:19:92:58:90:
(0)	E4:A2:35:77:3B:EF:92:E0:EB:8F:D4:9F:BF:49:BF:01:
(0)	C9:99:71:73:02:20:6C:6D:E2:9E:B3:AA:B2:EF:28:35:
(0)	2F:B4:CC:D6:96:8A:9C:DC:41:49:11:5E:13:04:7C:24:
(0)	22:55:8B:AF:3C:E3
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 56:14:06:9A:2F:D7:C2:EC:D3:F5:E1:BD:44:B2:3E:C7:
(0)	46:76:B9:BC:99:11:5C:C0:EF:94:98:55:D6:89:D0:DD

(0)	Timestamp : May 18 11:15:30.513 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:3C:A4:5A:84:5C:22:63:B2:4B:80:08:58:
(0)	39:09:CA:BD:21:6E:B6:82:B1:02:59:81:C0:41:2B:50:
(0)	B6:DB:FF:66:02:21:00:DB:50:07:D7:EE:31:2F:FF:EE:
(0)	8B:25:93:55:1B:34:69:52:85:A2:6A:54:3D:3D:3C:26:
(0)	30:5D:C8:41:30:18:B6
(0)Signature	(256 octets)
(0)	66:0e:56:73:ed:ab:74:cd:ae:a5:85:ba:9b:f0:18:89
(0)	15:8f:65:4a:05:c6:79:e0:03:28:d8:81:64:af:ef:8d
(0)	ca:35:48:b6:b7:d8:61:1e:bd:af:5a:34:ff:bb:41:e5
(0)	ff:4f:4e:09:c5:d9:a5:8d:4e:29:74:31:f8:a3:f4:d1
(0)	b9:de:96:82:57:77:bc:00:0b:5f:7c:61:8a:30:78:fd
(0)	00:f2:91:73:83:4e:cb:9e:9a:93:26:3d:97:09:9c:16
(0)	e1:e8:19:95:46:a2:8f:26:e5:56:b8:07:37:1d:74:ec
(0)	d3:16:2b:58:f4:07:3a:70:c5:e4:f6:0f:da:59:36:bd
(0)	61:04:c0:85:17:c8:5e:40:aa:e3:54:87:83:ea:6c:dc
(0)	42:fa:41:e9:5b:fc:04:5e:da:fc:1a:8d:28:72:c7:32
(0)	c2:f1:3a:ca:6b:a2:23:04:45:e6:4f:37:e9:7e:c6:4d
(0)	75:e8:e9:ba:7c:34:a7:7b:27:5e:89:c7:7c:7c:15:f1
(0)	2a:2f:5f:51:25:8a:9b:c6:e7:ab:45:4f:11:7f:cd:90
(0)	91:1a:2a:d8:06:35:f5:82:75:63:ad:c2:c4:16:88:b5
(0)	97:c2:f7:b7:eb:75:83:31:02:c2:ad:2d:c3:82:5d:3e
(0)	4c:6b:6c:2a:86:aa:8f:56:3e:8c:d5:c8:34:f1:51:f3
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:

(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

■□□□□ 1 HTTP Methods Returned by OPTIONS Request rdg.enterate.com:80/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Allow: OPTIONS, TRACE, GET, HEAD, POST

■□□□□ 1 HTTP Response Method and Header Information Collected rdg.enterate.com:80/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

```
GET / HTTP/1.0
Host: rdg.enterate.com
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 18 Jul 2018 01:38:31 GMT
Accept-Ranges: bytes
ETag: "f19c98381ed41:0"
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:39:18 GMT
Connection: keep-alive
Content-Length: 703
```

1 Referrer-Policy HTTP Security Header Not Detected rdg.enterate.com:80/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 80 port.

1 HTTP Strict Transport Security (HSTS) Support Detected rdg.enterate.com:80/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

1 List of Web Directories rdg.enterate.com:80/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/rpc/	brute force

1 Web Server Unconfigured - Default Install Page Present rdg.enterate.com:80/tcp

QID:	87089
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/28/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The web server uses its default welcome page.
This may mean that the web server is not used or is not properly configured.
QID Detection Logic (unauthenticated):
The Detection reviews the default page.

IMPACT:
N/A

SOLUTION:
Configure the web server to not display the default welcome page or disable the HTTP service if you do not use it.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 18 Jul 2018 01:38:31 GMT
Accept-Ranges: bytes
ETag: "f19c98381ed41:0"
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:39:18 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 HTTP Methods Returned by OPTIONS Request rdg.enterate.com:443/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

1 HTTP Response Method and Header Information Collected rdg.enterate.com:443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 443.

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 18 Jul 2018 01:38:31 GMT
Accept-Ranges: bytes
ETag: "f19c98381ed41:0"
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:41:43 GMT
Connection: keep-alive
Content-Length: 703
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected rdg.enterate.com:443/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 443 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected rdg.enterate.com:443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubdomains

1 List of Web Directories Requiring Authentication rdg.enterate.com:443/tcp

QID:	86671
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The service has identified a list of Web directories which require authentication to access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directories Requiring Authentication
/rpc/

1 List of Web Directories rdg.enterate.com:443/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/rpc/	brute force

■□□□□ 1 Web Server Unconfigured - Default Install Page Present rdg.enterate.com:443/tcp

QID:	87089
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/28/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The web server uses its default welcome page.
This may mean that the web server is not used or is not properly configured.
QID Detection Logic (unauthenticated):
The Detection reviews the default page.

IMPACT:
N/A

SOLUTION:
Configure the web server to not display the default welcome page or disable the HTTP service if you do not use it.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 18 Jul 2018 01:38:31 GMT
Accept-Ranges: bytes
ETag: "f19c98381ed41:0"
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:41:43 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
```

```
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:43:55 GMT
```

```
Connection: close
Content-Length: 315

       <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:44:09 GMT
Connection: close
Content-Length: 315

       <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected rdg.enterate.com:47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: rdg.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:43:55 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:46:14 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:46:27 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected rdg.enterate.com:5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: rdg.enterate.com:5985
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:46:14 GMT
Connection: close
Content-Length: 315
```

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH

ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

▮▯▯▯▯ 1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low

ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:

(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)

(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:

(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

Information Gathered (87)

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: web1.enterate.com
```

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 7239/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:

This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 7239.
GET / HTTP/1.0
Host: web1.enterate.com:7239
```

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2012 R2 Standard	CIFS via TCP Port 445	
Windows 2012 R2/8.1	NTLMSSP	
Windows Vista / Windows 2008	TCP/IP Fingerprint	U3423:80
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCOM System Activator	0.0	49154			
Microsoft Local Security Architecture	0.0	49155, 49171			
Microsoft LSA DS Access	0.0	49155, 49171			
Microsoft Network Logon	1.0	49155, 49171			
Microsoft Scheduler Control Service	1.0	49154			
Microsoft Security Account Manager	1.0	49155, 49171			
Microsoft Server Service	3.0	49154			
Microsoft Task Scheduler	1.0	49154			
MS Wbem Transport IEnumWbemClassObject	0.0	49154			
MS Wbem Transport IWbemLevel1Login	0.0	49154			
MS Wbem Transport IWbemObjectSink	0.0	49154			
MS Wbem Transport IWbemServices	0.0	49154			
(Unknown Service)	1.0	49155, 49171			

(Unknown Service)	0.0	49154
(Unknown Service)	1.0	49154
(Unknown Service)	4.0	49154
(Unknown Service)	0.0	49155, 49171
(Unknown Service)	1.0	49152

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 80, the host's uptime is 2 days, 22 hours, and 56 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Microsoft ASP.NET HTTP Handlers Enumerated port 80/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 80/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's
"Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

2 Microsoft ASP.NET HTTP Handlers Enumerated port 443/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 443/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").

Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,.Soap,

2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1
```

■■□□□ 2 Microsoft ASP.NET HTTP Handlers Enumerated port 7239/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
.Aspx,.Asmx,.Rem,.Soap,
```

■■□□□ 2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 7239/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's
"Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Web Server HTTP Protocol Versions port 7239/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 7239 port.GET / HTTP/1.1

▮▮▯▯▯ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

▮▯▯▯▯ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.30.20	web1.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 1, 7, 11.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2512,2514-2701,
2703-2868,2870-3388,3390-5630,5632-5984,5986-6128,6130-7238,7240-14967,
14969-40568,40570-42423,42425-47000,47002-49151,49156-49170,49172-49177,
49179,49181-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2392 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:16:59 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
web1.enterate.com	NTLM DNS
web1.enterate.com	FQDN
WEB1	NTLM NetBIOS

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:41:00
TCP	135	0:07:07
TCP	443	0:53:49
TCP	445	0:00:01
TCP	3389	0:00:51
TCP	5985	0:29:24
TCP	7239	0:46:50
TCP	47001	0:28:25
TCP	49152	0:05:05
TCP	49153	0:05:05
TCP	49154	0:05:05
TCP	49155	0:05:05
TCP	49171	0:05:05
TCP	49178	0:05:05
TCP	49180	0:05:22

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
7239	unknown	unknown	http over ssl	
47001	unknown	unknown	http	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	
49155	unknown	unknown	msrpc	
49171	unknown	unknown	msrpc	
49178	unknown	unknown	msrpc	
49180	unknown	unknown	msrpc	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:09 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

WEB1

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045

Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1066396211 with a standard deviation of 608187060. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5104 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 80: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 11 milli seconds
```

■□□□□ 1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:39:12 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 80/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
GET / HTTP/1.0

```
Host: web1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:39:36 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

```
GET / HTTP/1.0
Host: web1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:39:12 GMT
Connection: keep-alive
Content-Length: 701
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 80/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 80 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 80/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubdomains

■□□□□ 1 Microsoft IIS ASP.NET Version Obtained port 80/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
X-AspNet-Version: 4.0.30319
```

1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/portal/	brute force
/test/	brute force
/backups	brute force
/portal/	web page
/portal/images/	web page
/tmp/	brute force

/Portal/	brute force
/Portal/	web page
/Portal/images/	web page
/test/	web page

1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:43:24 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
```

```
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:44:20 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 443/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as

the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona

localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale

organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad

(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

1 HTTP Methods Returned by OPTIONS Request port 443/tcp

QID: 45056
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/16/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

1 HTTP Response Method and Header Information Collected port 443/tcp

QID: 48118
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/20/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 443.

```
GET / HTTP/1.0
Host: web1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:43:24 GMT
Connection: keep-alive
Content-Length: 701
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin

7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 443 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubdomains

1 Microsoft IIS ASP.NET Version Obtained port 443/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
X-AspNet-Version: 4.0.30319
```

1 List of Web Directories port 443/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/test/	brute force
/portal/	brute force
/backups	brute force

/tmp/	brute force
/portal/	web page
/portal/images/	web page
/Portal/	brute force
/test/	web page
/Portal/	web page
/Portal/images/	web page

1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:17 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:18 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: web1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:17 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 7239/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 7239/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 7239.

GET / HTTP/1.0
Host: web1.enterate.com:7239



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:59:52 GMT
Connection: keep-alive
Content-Length: 701
```

1 Referrer-Policy HTTP Security Header Not Detected port 7239/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 7239 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 7239/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubdomains

■□□□□ 1 Microsoft IIS ASP.NET Version Obtained port 7239/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

X-AspNet-Version: 4.0.30319

■□□□□ 1 List of Web Directories port 7239/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/stats/	brute force

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com:47001


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:13 GMT
Connection: close
Content-Length: 315
```

```
        <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:14 GMT
Connection: close
Content-Length: 315

        <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: web1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:13 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 7239/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com:7239



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:59:52 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 7239/tcp over SSL

QID: 13910

Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web1.enterate.com:7239



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 06:00:46 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 SSL Server Information Retrieval port 7239/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM

ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384 AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256 AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256 AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED				

1 SSL Session Caching Information port 7239/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 7239/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 7239/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low

ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 7239/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 7239/tcp over SSL

QID:	38717
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 7239/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 7239/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 7239/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:

(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)

(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:

(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

▮▯▯▯▯ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮▯▯▯▯ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to

establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1

(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2

(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/

(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.16.30.21 (app1.enterate.com, APP1) Windows 2012 R2 Standard

Potential Vulnerabilities (4)

■■■□□ 3 Service Stopped Responding port 61199/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:

The service/daemon is vulnerable to a denial of service attack.

SOLUTION:

This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
3 consecutive connection attempts failed after a total number of 5 successful connections.

■■■□□ 3 Service Stopped Responding port 3820/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:
The service/daemon is vulnerable to a denial of service attack.

SOLUTION:
This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
3 consecutive connection attempts failed after a total number of 55 successful connections.

■■■□□ 3 Service Stopped Responding port 8686/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:
The service/daemon is vulnerable to a denial of service attack.

SOLUTION:
This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
3 consecutive connection attempts failed after a total number of 1 successful connections.

🟨🟨🟨□□ 3 Service Stopped Responding port 3920/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:
The service/daemon is vulnerable to a denial of service attack.

SOLUTION:
This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
3 consecutive connection attempts failed after a total number of 48 successful connections.
```

Information Gathered (83)

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: app1.enterate.com
```

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2012 R2 Standard	CIFS via TCP Port 445	
Windows 2012 R2/8.1	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U6483:135

■■□□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Message Queuing - QM2QM V1	1.0	2105, 2103, 2107, 49175			
Message Queuing - QMRT V1	1.0	2105, 2103, 2107, 49175			
Message Queuing - QMRT V2	1.0	2105, 2103, 2107, 49175			
Message Queuing - RemoteRead V1	1.0	2105, 2103, 2107, 49175			
Microsoft Local Security Architecture	0.0	49169, 49155			
Microsoft LSA DS Access	0.0	49169, 49155			
Microsoft Network Logon	1.0	49169, 49155			
Microsoft Scheduler Control Service	1.0	49154			
Microsoft Security Account Manager	1.0	49169, 49155			
Microsoft Server Service	3.0	49154			
Microsoft Task Scheduler	1.0	49154			
MS Wbem Transport IEnumWbemClassObject	0.0	49154			
MS Wbem Transport IWbemObjectSink	0.0	49154			
MS Wbem Transport IWbemServices	0.0	49154			
(Unknown Service)	1.0	49169, 49155			
(Unknown Service)	0.0	2105, 49154, 2103, 2107, 49175			
(Unknown Service)	0.0	49154			
(Unknown Service)	1.0	2105, 2103, 2107, 49175			
(Unknown Service)	1.0	49154			
(Unknown Service)	0.0	49169, 49155			
(Unknown Service)	4.0	49154			
(Unknown Service)	1.0	49152			

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 139, the host's uptime is 2 days, 21 hours, and 48 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

■■□□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe.
Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■■□□□ 2 Microsoft ASP.NET HTTP Handlers Enumerated port 443/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 443/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
.Aspx,.Asmx,.Rem,.Soap,
```

■■□□□ 2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

2 Microsoft ASP.NET HTTP Handlers Enumerated port 85/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 85/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").

Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Web Server HTTP Protocol Versions port 85/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 85 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.30.21	app1.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 1, 7.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-84,86-134,136-138,140-442,444,446-1705,1707-1800,1802-1999,2001-2102,
2104,2106,2108-2146,2148-2512,2514-2701,2703-2868,2870-3388,3390-3699,
3701-3819,3821-3919,3921-4847,4849-5630,5632-5984,5986-6128,6130-7675,
7677-8079,8081-8180,8182-8685,8687-42423,42425-47000,47002-49151,49156-49168,
49170-49174,49177,49179-56840,56842-61194,61196-61197,61200-64026,64028-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2841 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:24:28 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
app1.enterate.com	NTLM DNS
app1.enterate.com	FQDN
APP1	NTLM NetBIOS

■□□□□ 1 Java Remote Method Invocation Detected

QID:	45186
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/23/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Java Remote Method Invocation or Java RMI, is a mechanism that allows one to invoke a method on an object that exists in another address space.
Java RMI is running on target host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Service name: Java RMI is running on TCP port 61195.

■□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

1 Scan Activity per Port

QID:	45426

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	85	0:37:34
TCP	135	0:07:35
TCP	139	0:01:05
TCP	443	0:47:48
TCP	3389	0:00:56
TCP	3700	0:00:47
TCP	3820	0:07:17
TCP	3920	0:11:08
TCP	4848	0:12:46
TCP	5985	0:29:59
TCP	7676	0:00:03
TCP	8080	0:11:19
TCP	8181	0:17:12
TCP	8686	0:04:49
TCP	47001	0:44:07
TCP	49152	0:05:08
TCP	49153	0:05:05
TCP	49154	0:05:15
TCP	49155	0:05:08
TCP	49169	0:05:05
TCP	49175	0:05:05
TCP	49176	0:05:42
TCP	49178	0:05:05
TCP	61195	0:05:27
TCP	61198	0:10:13

TCP	61199	0:05:54

1 Oracle JMS Open Message Queue Detected

QID:	48154
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/16/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Oracle JMS Open Message Queue is running on the remote host.

QID Detection Logic:(Unauthenticated)
This QID gets the Openmq version from the provided banner.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Oracle JMS Open Message Queue Detected on port - 7676

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
85	mit-ml-dev	MIT ML Device	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1801	msmq	Microsoft Message Que	Microsoft Message Queue Server	
2103	zephyr-clt	Zephyr serv-hm connection	msrpc	
2105	minipay	MiniPay	msrpc	
2107	unknown	unknown	msrpc	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
3700	portal of doom	portal_of_doom backdoor	GIOP	
3820	unknown	unknown	unknown	
3920	unknown	unknown	unknown	
4848	unknown	unknown	unknown	
5985	unknown	unknown	http	
7676	unknown	unknown	OPENMQ	
8080	http-alt	HTTP Alternate (see port 80)	http	
8181	IpSwitch-IMail-WebStatus	IpSwitch-IMail-WebStatus	http over ssl	
8686	unknown	unknown	unknown	
47001	unknown	unknown	http	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	

49155	unknown	unknown	msrpc
49169	unknown	unknown	msrpc
49175	unknown	unknown	msrpc
49176	unknown	unknown	msrpc
49178	unknown	unknown	msrpc
61195	unknown	unknown	RMIRegistry
61198	unknown	unknown	unknown
61199	unknown	unknown	unknown

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:09 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

APP1

■□□□□ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1192977030 with a standard deviation of 632463181. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5255 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046

Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 15 milli seconds
```

■□□□□ 1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:40:23 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:41:18 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
```

</html>

1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 443/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:

(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:

(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

■□□□□ 1 Default Web Page port 8080/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:8080



HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1  Java/Oracle Corporation/1.8)
Accept-Ranges: bytes
ETag: W/"4626-1536340331348"
Last-Modified: Fri, 07 Sep 2018 17:12:11 GMT
Content-Type: text/html
Date: Sat, 20 Feb 2021 05:38:50 GMT
Connection: keep-alive
Content-Length: 4626

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 2010, 2014 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
 body{margin-top:0}
 body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
 h1 {font-size:18pt}
 h2 {font-size:14pt}
 h3 {font-size:12pt}
 code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
 li {padding-bottom: 8px}
 p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
 p.copy {text-align: center}
 table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
 th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
 td.insidehead {font-weight:bold; background:white; text-align: left;}
 a {text-decoration:none; color:#3E6B8A}
 a:visited{color:#917E9C}
 a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0" cellspacing="0"
cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993">       <font color="#ffffff"> <b>GlassFish Server</b></font>       </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The document root folder for this
server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a href="http://localhost:4848">go to the
```

```
Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a href="http://www.oracle.com/support/premier/index.html">Oracle Premier
Support for Software</a>. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT
investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional technologies and
frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a href="http://wikis.oracle.com/display/GlassFish/
UsageMetrics">GlassFish Server usage</a> that is transmitted by the Update Tool installer as part of the automatic update processes. No
personally identifiable information is collected by this process.</p>
-->
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a>  page for information about how to join the GlassFish community. The
GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of
the Java&trade; Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see  <var>as-install</var><code>/docs/about.
html</code>, where <var>as-install</var> is the GlassFish Server installation directory.</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a href="http://www.oracle.com/corporate/contact/">Contact</
a>   |
Copyright © 2010, 2014 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p></body></html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8080/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:8080



HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1  Java/Oracle Corporation/1.8)
Accept-Ranges: bytes
ETag: W/"4626-1536340331348"
Last-Modified: Fri, 07 Sep 2018 17:12:11 GMT
Content-Type: text/html
Date: Sat, 20 Feb 2021 05:38:50 GMT
Connection: keep-alive
Content-Length: 4626

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 2010, 2014 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
 body{margin-top:0}
 body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
 h1 {font-size:18pt}
 h2 {font-size:14pt}
 h3 {font-size:12pt}
 code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
 li {padding-bottom: 8px}
 p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
 p.copy {text-align: center}
 table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
 th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
 td.insidehead {font-weight:bold; background:white; text-align: left;}
 a {text-decoration:none; color:#3E6B8A}
 a:visited{color:#917E9C}
 a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0" cellspacing="0"
cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993">       <font color="#ffffff"> <b>GlassFish Server</b></font>       </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The document root folder for this
server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a href="http://localhost:4848">go to the
Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a href="http://www.oracle.com/support/premier/index.html">Oracle Premier
Support for Software</a>. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT
investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional technologies and
frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
```

```
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a href="http://wikis.oracle.com/display/GlassFish/
UsageMetrics">GlassFish Server usage</a> that is transmitted by the Update Tool installer as part of the automatic update processes. No
personally identifiable information is collected by this process.</p>
-->
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a>  page for information about how to join the GlassFish community. The
GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of
the Java&trade; Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see  <var>as-install</var><code>/docs/about.
html</code>, where <var>as-install</var> is the GlassFish Server installation directory.</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a href="http://www.oracle.com/corporate/contact/">Contact</
a>   |
Copyright © 2010, 2014 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p></body></html>
```

■□□□□ 1 Web Server Version port 8080/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/03/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
GlassFish Server Open Source Edition 4.1	_

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:43:06 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:43:20 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: app1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:43:06 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 443/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 443.

```
GET / HTTP/1.0
Host: app1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:40:23 GMT
Connection: keep-alive
Content-Length: 701
```

▮▯▯▯▯ 1 Referrer-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 443 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

■□□□□ 1 Microsoft IIS ASP.NET Version Obtained port 443/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
X-AspNet-Version: 4.0.30319
```

■□□□□ 1 List of Web Directories port 443/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/aspnet_client/	brute force

■□□□□ 1 Default Web Page port 85/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:85



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:45:25 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
```

```
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 85/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:85



HTTP/1.1 200 OK
Content-Type: text/html
```

```
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:46:46 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 85/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: OPTIONS, TRACE, GET, HEAD, POST

1 HTTP Response Method and Header Information Collected port 85/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 85.

```
GET / HTTP/1.0
Host: app1.enterate.com:85


HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
```

```
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:45:25 GMT
Connection: keep-alive
Content-Length: 701
```

▮▯▯▯▯ 1 Referrer-Policy HTTP Security Header Not Detected port 85/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 85 port.

▮▯▯▯▯ 1 HTTP Strict Transport Security (HSTS) Support Detected port 85/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

1 Microsoft IIS ASP.NET Version Obtained port 85/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
X-AspNet-Version: 4.0.30319
```

1 List of Web Directories port 85/tcp

QID:	86672
Category:	Web server

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/aspnet_client/	brute force

■□□□□ 1 Default Web Page port 8181/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:8181
```

```
HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1  Java/Oracle Corporation/1.8)
Accept-Ranges: bytes
ETag: W/"4626-1536340331348"
Last-Modified: Fri, 07 Sep 2018 17:12:11 GMT
Content-Type: text/html
Date: Sat, 20 Feb 2021 05:45:11 GMT
Connection: keep-alive
Content-Length: 4626

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 2010, 2014 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
 body{margin-top:0}
 body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
 h1 {font-size:18pt}
 h2 {font-size:14pt}
 h3 {font-size:12pt}
 code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
 li {padding-bottom: 8px}
 p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
 p.copy {text-align: center}
 table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
 th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
 td.insidehead {font-weight:bold; background:white; text-align: left;}
 a {text-decoration:none; color:#3E6B8A}
 a:visited{color:#917E9C}
 a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0" cellspacing="0"
cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993">       <font color="#ffffff"> <b>GlassFish Server</b></font>       </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The document root folder for this
server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a href="http://localhost:4848">go to the
Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a href="http://www.oracle.com/support/premier/index.html">Oracle Premier
Support for Software</a>. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT
investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional technologies and
frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a href="http://wikis.oracle.com/display/GlassFish/
UsageMetrics">GlassFish Server usage</a> that is transmitted by the Update Tool installer as part of the automatic update processes. No
personally identifiable information is collected by this process.</p>
-->
```

```
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a>  page for information about how to join the GlassFish community. The
GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of
the Java&trade; Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see  <var>as-install</var><code>/docs/about.
html</code>, where <var>as-install</var> is the GlassFish Server installation directory.</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a href="http://www.oracle.com/corporate/contact/">Contact</
a>   |
Copyright © 2010, 2014 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p></body></html>
```

▮▯▯▯▯ 1 Default Web Page (Follow HTTP Redirection) port 8181/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:8181



HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1  Java/Oracle Corporation/1.8)
Accept-Ranges: bytes
ETag: W/"4626-1536340331348"
Last-Modified: Fri, 07 Sep 2018 17:12:11 GMT
Content-Type: text/html
Date: Sat, 20 Feb 2021 05:45:11 GMT
Connection: keep-alive
Content-Length: 4626

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.
```

```
Copyright (c) 2010, 2014 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
 body{margin-top:0}
 body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
 h1 {font-size:18pt}
 h2 {font-size:14pt}
 h3 {font-size:12pt}
 code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
 li {padding-bottom: 8px}
 p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
 p.copy {text-align: center}
 table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
 th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
 td.insidehead {font-weight:bold; background:white; text-align: left;}
 a {text-decoration:none; color:#3E6B8A}
 a:visited{color:#917E9C}
 a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0" cellspacing="0"
cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993">      <font color="#ffffff"> <b>GlassFish Server</b></font>      </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The document root folder for this
server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a href="http://localhost:4848">go to the
Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a href="http://www.oracle.com/support/premier/index.html">Oracle Premier
Support for Software</a>. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT
investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional technologies and
frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a href="http://wikis.oracle.com/display/GlassFish/
UsageMetrics">GlassFish Server usage</a> that is transmitted by the Update Tool installer as part of the automatic update processes. No
personally identifiable information is collected by this process.</p>
-->
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a>  page for information about how to join the GlassFish community. The
GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of
the Java&trade; Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see  <var>as-install</var><code>/docs/about.
html</code>, where <var>as-install</var> is the GlassFish Server installation directory.</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a href="http://www.oracle.com/corporate/contact/">Contact</
a>   |
Copyright © 2010, 2014 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p></body></html>
```

▮▯▯▯▯ 1 SSL Server Information Retrieval port 8181/tcp over SSL

QID:	38116
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8181/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 8181/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8181/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	sect409r1	409	yes	204	low

ECDHE	sect409k1	409	yes	204	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low

1 SSL/TLS Protocol Properties port 8181/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8181/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate.
Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8181/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8181/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption

(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:

(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	

countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2

(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	0 (0x0)
(2)Signature Algorithm	sha256WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)Valid From	Sep 1 00:00:00 2009 GMT
(2)Valid Till	Dec 31 23:59:59 2037 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(2048 bit)
(2)	RSA Public-Key: (2048 bit)
(2)	Modulus:
(2)	00:bf:71:62:08:f1:fa:59:34:f7:1b:c9:18:a3:f7:
(2)	80:49:58:e9:22:83:13:a6:c5:20:43:01:3b:84:f1:
(2)	e6:85:49:9f:27:ea:f6:84:1b:4e:a0:b4:db:70:98:
(2)	c7:32:01:b1:05:3e:07:4e:ee:f4:fa:4f:2f:59:30:
(2)	22:e7:ab:19:56:6b:e2:80:07:fc:f3:16:75:80:39:
(2)	51:7b:e5:f9:35:b6:74:4e:a9:8d:82:13:e4:b6:3f:
(2)	a9:03:83:fa:a2:be:8a:15:6a:7f:de:0b:c3:b6:19:
(2)	14:05:ca:ea:c3:a8:04:94:3b:46:7c:32:0d:f3:00:
(2)	66:22:c8:8d:69:6d:36:8c:11:18:b7:d3:b2:1c:60:
(2)	b4:38:fa:02:8c:ce:d3:dd:46:07:de:0a:3e:eb:5d:
(2)	7c:c8:7c:fb:b0:2b:53:a4:92:62:69:51:25:05:61:
(2)	1a:44:81:8c:2c:a9:43:96:23:df:ac:3a:81:9a:0e:
(2)	29:c5:1c:a9:e9:5d:1e:b6:9e:9e:30:0a:39:ce:f1:
(2)	88:80:fb:4b:5d:cc:32:ec:85:62:43:25:34:02:56:
(2)	27:01:91:b4:3b:70:2a:3f:6e:b1:e8:9c:88:01:7d:
(2)	9f:d4:f9:db:53:6d:60:9d:bf:2c:e7:58:ab:b8:5f:
(2)	46:fc:ce:c4:1b:03:3c:09:eb:49:31:5c:69:46:b3:
(2)	e0:47
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Basic Constraints	critical

(2)	CA:TRUE
(2)X509v3 Key Usage	critical
(2)	Certificate Sign, CRL Sign
(2)X509v3 Subject Key Identifier	3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(2)Signature	(256 octets)
(2)	99:db:5d:79:d5:f9:97:59:67:03:61:f1:7e:3b:06:31
(2)	75:2d:a1:20:8e:4f:65:87:b4:f7:a6:9c:bc:d8:e9:2f
(2)	d0:db:5a:ee:cf:74:8c:73:b4:38:42:da:05:7b:f8:02
(2)	75:b8:fd:a5:b1:d7:ae:f6:d7:de:13:cb:53:10:7e:8a
(2)	46:d1:97:fa:b7:2e:2b:11:ab:90:b0:27:80:f9:e8:9f
(2)	5a:e9:37:9f:ab:e4:df:6c:b3:85:17:9d:3d:d9:24:4f
(2)	79:91:35:d6:5f:04:eb:80:83:ab:9a:02:2d:b5:10:f4
(2)	d8:90:c7:04:73:40:ed:72:25:a0:a9:9f:ec:9e:ab:68
(2)	12:99:57:c6:8f:12:3a:09:a4:bd:44:fd:06:15:37:c1
(2)	9b:e4:32:a3:ed:38:e8:d8:64:f3:2c:7e:14:fc:02:ea
(2)	9f:cd:ff:07:68:17:db:22:90:38:2d:7a:8d:d1:54:f1
(2)	69:e3:5f:33:ca:7a:3d:7b:0a:e3:ca:7f:5f:39:e5:e2
(2)	75:ba:c5:76:18:33:ce:2c:f0:2f:4c:ad:f7:b1:e7:ce
(2)	4f:a8:c4:9b:4a:54:06:c5:7f:7d:d5:08:0f:e2:1c:fe
(2)	7e:17:b8:ac:5e:f6:d4:16:b2:43:09:0c:4d:f6:a7:6b
(2)	b4:99:84:65:ca:7a:88:e2:e2:44:be:5c:f7:ea:1c:f5

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:47001
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:57:29 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: app1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:00:12 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: app1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:57:29 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Web Server Version port 8181/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/14/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
GlassFish Server Open Source Edition 4.1	_

▮□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					

TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes

Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

▮▯▯▯▯ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT

(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:

(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2

(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.16.30.22 (web2.enterate.com, WEB2) Windows 2012 R2 Standard

Potential Vulnerabilities (1)

■□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (40)

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2012 R2 Standard	CIFS via TCP Port 445	
Windows 2012 R2/8.1	NTLMSSP	
Windows Vista / Windows 2008	TCP/IP Fingerprint	U3423:80

▮▮▯▯▯ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Microsoft Local Security Architecture	0.0	49174, 49155			
Microsoft LSA DS Access	0.0	49174, 49155			
Microsoft Network Logon	1.0	49174, 49155			
Microsoft Scheduler Control Service	1.0	49154			
Microsoft Security Account Manager	1.0	49174, 49155			
Microsoft Server Service	3.0	49154			
Microsoft Task Scheduler	1.0	49154			
MS Wbem Transport IEnumWbemClassObject	0.0	49154			
MS Wbem Transport IWbemObjectSink	0.0	49154			
MS Wbem Transport IWbemServices	0.0	49154			
(Unknown Service)	1.0	49174, 49155			
(Unknown Service)	0.0	49154			
(Unknown Service)	1.0	49154			
(Unknown Service)	0.0	49174, 49155			
(Unknown Service)	4.0	49154			
(Unknown Service)	1.0	49152			

■■□□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 80, the host's uptime is 3 days, 15 hours, and 2 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe.
Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1
```

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.30.22	web2.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 1, 7, 11.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2512,2514-2701,
2703-2868,2870-3388,3390-5630,5632-5984,5986-6128,6130-42423,42425-47000,
47002-49151,49156-49173,49175-49177,49180-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2351 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:16:18 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
web2.enterate.com	NTLM DNS
web2.enterate.com	FQDN
WEB2	NTLM NetBIOS

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:

Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.
```

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:47:36
TCP	135	0:07:22
TCP	443	0:03:05
TCP	3389	0:00:52
TCP	5985	0:32:42
TCP	47001	0:28:52
TCP	49152	0:05:05
TCP	49153	0:05:05
TCP	49154	0:05:05
TCP	49155	0:05:05
TCP	49174	0:05:06
TCP	49178	0:05:05
TCP	49179	0:05:05

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)

Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the

Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	unknown	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
47001	unknown	unknown	http	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	
49155	unknown	unknown	msrpc	
49174	unknown	unknown	msrpc	
49178	unknown	unknown	msrpc	
49179	unknown	unknown	msrpc	

■□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:10 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

WEB2

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1058214757 with a standard deviation of 781315887. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5113 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 80: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Duration: 10 milli seconds

■□□□□ 1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web2.enterate.com



<head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a HREF="https://web2.enterate.com/">here</a></body>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

```
GET / HTTP/1.0
Host: web2.enterate.com



HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: https://web2.enterate.com/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:38:27 GMT
Connection: keep-alive
Content-Length: 149
```

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 80/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubdomains

■□□□□ 1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/admin/	web page
/help/	web page
/install/	web page
/secure/	web page
/manager/	web page

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:43:09 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:43:41 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: web2.enterate.com:5985
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:43:09 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:45:21 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: web2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:45:36 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:

This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: web2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:45:21 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

▮□□□□ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

▮□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as

the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona

localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale

organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad

(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.16.50.90 (-, NAS16-1)

Vulnerabilities (4)

■■■□□ 3 WINS Domain Controller Spoofing Vulnerability - Zero Day

QID:	70007
Category:	SMB / NETBIOS
CVE ID:	CVE-1999-1593
Vendor Reference:	-
Bugtraq ID:	2221
Service Modified:	02/08/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Windows Internet Naming Service (WINS) ships with Microsoft Windows NT Server and is also supported by Samba server. WINS resolves IP addresses with network computer names in a client to server environment. A distributed database is updated with an IP address for every machine available on the network. Unfortunately, WINS does not properly verify the registration of Domain Controllers (DCs).
It's possible for a user to modify the entries for a domain controller, causing the WINS service to redirect requests for the DC to another system. This can lead to a loss of network functionality for the domain. The DC impersonator can also be set up to capture username and password hashes passed to it during login attempts.

IMPACT:

By exploting this vulnerability, an unauthorized user can cause the WINS service to redirect requests for a domain controller to a different system, which could lead to a loss of network functionality. The user may also be able to retrieve username and password hashes.

SOLUTION:

There are no vendor supplied patches available at this time.
Workaround:
The following workaround was provided by David Byrne <dbyrne@tiaa-cref.org>:

> The best workaround I could think of is to use static entries for records
> that are sensitive (there are probably more besides 1Ch). Domain Controllers
> shouldn't be changed very often, so the management work would be minimal.

The following workaround was provided by Paul L Schmehl <pauls@utdallas.edu>:

> MS's response was that because WINS uses NetBIOS, which has no security
> capabilities, there was no way to prevent that sort of hijacking. Their
> answer is Active Directory, Kerberos and DNS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Found through udp port 137

■■■□□ 3 NetBIOS Name Conflict Vulnerability

QID:	70008
Category:	SMB / NETBIOS
CVE ID:	CVE-2000-0673
Vendor Reference:	MS00-047
Bugtraq ID:	1514, 1515
Service Modified:	03/17/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A malicious user can send a NetBIOS Name Conflict message to the NetBIOS name service even when the receiving machine is not in the process of registering its NetBIOS name. As a result, the target will not attempt to use that name in any future network connection attempts, which could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.
This is a design flaw problem in the NetBIOS protocol and the WINS dynamic name registration, which is present whenever WINS is supported.

IMPACT:

If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.

SOLUTION:

The best workaround for Microsoft Windows and Samba Server is to block all incoming traffic from the Internet to UDP ports 137 and 138.
For Windows platforms, microsoft has released some patches to address this issue.
Microsoft has released a patch (Hotfix 269239). After the patch is applied, conflict messages will only be responded to during the initial name registration process. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047) (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-047.asp).
Hotfix 269239 mitigates the issue by generating log events for detected
name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable. Microsoft acknowledges this problem in their documentation for Hotfix 269239.
The following is a list of Microsoft patches:
Microsoft Windows NT 4.0 patch Q269239i (http://www.microsoft.com/downloads/release.asp?ReleaseID=22138)
Microsoft Windows NT Terminal Server patch Q269239i (http://www.microsoft.com/downloads/release.asp?ReleaseID=24516)
Microsoft Windows 2000 patch Q269239_W2K_SP2_x86_en (http://download.microsoft.com/download/win2000platform/Patch/q269239/NT5/EN-US/Q269239_W2K_SP2_x86_en.EXE)
For Samba there are no vendor supplied patches available at this time.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2000-0673
Description:	Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict - The Exploit-DB Ref : 20106
Link:	http://www.exploit-db.com/exploits/20106

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Found through udp port 137

■■■□□ 3 NetBIOS Release Vulnerability

QID:	70009
Category:	SMB / NETBIOS
CVE ID:	CVE-2000-0673
Vendor Reference:	MS00-047

Bugtraq ID:	1515, 1514
Service Modified:	03/17/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
A malicious user can send a NetBIOS Release message to a NetBIOS name service.

IMPACT:
If successfully exploited, the receiving machine is forced to place its name in conflict so that it will no longer be able to use it.

SOLUTION:
This is the correct protocol behavior. The best workaround for Microsoft Windows and Samba servers is to block all incoming traffic from the Internet to UDP ports 137 and 138.
Also for Windows, Microsoft has released a patch (Hotfix 269239), which adds a registry key that disables the NetBIOS name service from paying attention to these messages. For more information on this vulnerability and the patch, read Microsoft Security Bulletin (MS00-047) (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-047.asp).
Hotfix 269239 mitigates the issue by generating log events for detected name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable.
Microsoft acknowledges this problem in their documentation for Hotfix 269239.
The following is a list of Microsoft patches:
Microsoft Windows 2000 (Professional, Server, and Advanced Server) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23370)
Microsoft Windows NT 4.0 (Workstation, Server, and Server, Enterprise Edition) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22138)
Microsoft Windows NT Server 4.0 (Terminal Server Edition) Patch (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24516)
Windows 2003 inherently supports the registry value for ignoring Name release mentioned in the MS00-047 document. Please refer the document MS00-047 for information on configuring this registry value.
For Samba server there are no vendor supplied patches available at this time.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
The Exploit-DB

Reference:	CVE-2000-0673
Description:	Microsoft Windows NT 4.0/2000 - NetBIOS Name Conflict - The Exploit-DB Ref : 20106
Link:	http://www.exploit-db.com/exploits/20106

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Found through udp port 137

■■□□□ 2 NetBIOS Name Accessible

QID:	70000
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/28/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Unauthorized users can obtain this host's NetBIOS server name from a remote system.

IMPACT:

Unauthorized users can obtain the list of NetBIOS servers on your network. This list outlines trust relationships between server and client computers. Unauthorized users can therefore use a vulnerable host to penetrate secure servers.

SOLUTION:
If the NetBIOS service is not required on this host, disable it. Otherwise, block any NetBIOS traffic at your network boundaries.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
NAS16-1

Potential Vulnerabilities (3)

■■■□ 3 Service Stopped Responding port 80/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:
The service/daemon is vulnerable to a denial of service attack.

SOLUTION:
This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
3 consecutive connection attempts failed after a total number of 0 successful connections.

■■■□ 3 Service Stopped Responding port 443/tcp

QID:	38229

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:

The service/daemon is vulnerable to a denial of service attack.

SOLUTION:

This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

3 consecutive connection attempts failed after a total number of 0 successful connections.

■□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.

Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 80.
Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (11)

3 NetBIOS Bindings Information

QID:	70004
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following bindings were detected on this computer. Bindings have many purposes. They reflect such things as users logged-in, registration of a user name, registration of a service in a domain, and registering of a NetBIOS name.

IMPACT:

Unauthorized users can use this information in further attacks against the host. A list of logged-in users on the target host/network can potentially be used to launch social engineering attacks.

SOLUTION:

This service uses the UDP and TCP port 137. Typically, this port should not be
accessible to external networks, and should be firewalled.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Name	Service	NetBIOS Suffix

NAS16-1	Workstation Service	0x0
NAS16-1	Messenger Service Server (Machine or Logged-in User Name)	0x3
NAS16-1	File Server Service	0x20
WORKGROUP	Domain Name	0x0
WORKGROUP	Browser Service Elections	0x1e

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.50.90	No registered hostname

■□□□□ 1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	172.16.1.1	1.43ms	ICMP	
2	172.16.50.90	0.40ms	ICMP	

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2444 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:17:23 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
NAS16-1	NetBIOS

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:02:23
TCP	443	0:02:23
UDP	68	0:00:07
UDP	123	0:00:19
UDP	137	0:00:47
UDP	138	0:00:07

■□□□□ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
68	bootpc	Bootstrap Protocol Client	unknown
123	ntp	Network Time Protocol	unknown
137	netbios-ns	NETBIOS Name Service	netbios ns
138	netbios-dgm	NETBIOS Datagram Service	unknown

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	unknown	
443	https	http protocol over TLS/SSL	unknown	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:39:29 GMT
Unreachable (type=3 code=3)	UDP Port 12345	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 24250	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 2049	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1243	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 4590	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 9872	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 456	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 858	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 54047	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable

■□□□□ 1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAS16-1

1 NetBIOS Workgroup Name Detected

QID:	82062
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/02/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS workgroup or domain name for this system has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
WORKGROUP
```

172.16.50.100 (-, -)

Potential Vulnerabilities (2)

3 Service Stopped Responding port 80/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:

The service/daemon is vulnerable to a denial of service attack.

SOLUTION:

This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

3 consecutive connection attempts failed after a total number of 0 successful connections.

🟨□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 22.
Service name: Unknown - Possible Scan Interference on TCP port 80.

Information Gathered (10)

■■■□□ 3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/23/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Service name: SNMP on UDP port 161.

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.50.100	No registered hostname

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 11, 67, 1524, 1723, 2049, 2764.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
2-6,8-19,24,26-52,54-78,81-109,112,114-134,136-138,140-142,144-381,383-442,
444,446-512,514-911,913-1026,1030-1079,1081-1520,1522-1559,1561-1705,
```

1707-1721,1723-1999,2001-2033,2035,2037-2100,2102-2146,2148-2512,2514-2701,
2703-2868,2870-3127,3129-3388,3390-5491,5493-5504,5506-5549,5551-5559,
5561-5569,5571-5579,5581-5630,5632-5999,6001-6013,6015-6128,6130-7006,
7008-7009,7011-8079,8081-9098,9100-9989,9991-10109,10111-24566,24568-32770,
32772-42423,42425-48761,48763-65535

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	172.16.1.1	2.35ms	ICMP	
2	172.16.50.100	0.28ms	ICMP	

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2533 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:19:20 GMT

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	22	0:02:05
TCP	80	0:02:23
UDP	123	0:00:19
UDP	161	0:03:12

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
161	snmp	SNMP	snmp

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	unknown	
80	www-http	World Wide Web HTTP	unknown	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 1054	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 11117	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 512	Port Unreachable

Unreachable (type=3 code=3)	UDP Port 51100	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 135	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1981	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1434	Port Unreachable

1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

172.16.50.101 (-, -)

Potential Vulnerabilities (2)

3 Service Stopped Responding port 80/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:
The service/daemon is vulnerable to a denial of service attack.

SOLUTION:

This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

3 consecutive connection attempts failed after a total number of 0 successful connections.

1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 22.
Service name: Unknown - Possible Scan Interference on TCP port 80.

Information Gathered (10)

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/23/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Service name: SNMP on UDP port 161.

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.50.101	No registered hostname

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 67, 79, 2049, 2764, 3128.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
2-6,8-10,12-19,24,26-52,54-79,81-109,112,114-134,136-138,140-142,144-381,
383-442,444,446-512,514-911,913-1026,1030-1079,1081-1520,1522-1523,1525-1559,
1561-1705,1707-1721,1724-1999,2001-2033,2035,2037-2100,2102-2146,2148-2512,
2514-2701,2703-2868,2870-3388,3390-5491,5493-5504,5506-5549,5551-5559,
5561-5569,5571-5579,5581-5630,5632-5999,6001-6013,6015-6128,6130-7006,
```

7008-7009,7011-8079,8081-9098,9100-9989,9991-10109,10111-24566,24568-32770,
32772-42423,42425-48761,48763-65535

■□□□□ 1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	172.16.1.1	1.03ms	ICMP	
2	172.16.50.101	0.45ms	ICMP	

■□□□□ 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2531 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:19:18 GMT

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	22	0:02:10
TCP	80	0:02:23
UDP	123	0:00:19
UDP	161	0:03:12

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
161	snmp	SNMP	snmp

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	unknown	
80	www-http	World Wide Web HTTP	unknown	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Unreachable (type=3 code=3)	UDP Port 1054	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 512	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 51100	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 135	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1981	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1434	Port Unreachable

Unreachable (type=3 code=3)	UDP Port 61466	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7000	Port Unreachable
Echo (type=0 code=0)	Echo Request	Echo Reply

■□□□□ 1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

172.16.50.102 (-, -)

Potential Vulnerabilities (2)

■■■□□ 3 Service Stopped Responding port 80/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:
The service/daemon is vulnerable to a denial of service attack.

SOLUTION:
This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).

If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
3 consecutive connection attempts failed after a total number of 0 successful connections.

1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:
If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:
Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 22.
Service name: Unknown - Possible Scan Interference on TCP port 80.

Information Gathered (10)

■■■□□ 3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/23/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: SNMP on UDP port 161.

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.16.50.102	No registered hostname

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 11, 67, 1723, 2049, 2764.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
2-6,8-19,24,26-52,54-78,81-109,112,114-134,136-138,140-142,144-381,383-442,
444,446-512,514-911,913-1026,1030-1079,1081-1520,1522-1523,1525-1559,
1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,2102-2146,2148-2512,
2514-2701,2703-2868,2870-3127,3129-3388,3390-5491,5493-5504,5506-5549,
5551-5559,5561-5569,5571-5579,5581-5630,5632-5999,6001-6013,6015-6128,
6130-7006,7008-7009,7011-8079,8081-9098,9100-9989,9991-10109,10111-24566,

24568-32770,32772-42423,42425-48761,48763-65535

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	172.16.1.1	1.64ms	ICMP	
2	172.16.50.102	0.46ms	ICMP	

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2537 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:19:24 GMT

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	22	0:02:05
TCP	80	0:02:23
UDP	123	0:00:19
UDP	161	0:03:12

1 Open UDP Services List

QID:	82004

Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	unknown
161	snmp	SNMP	snmp

▮▯▯▯▯ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	unknown	
80	www-http	World Wide Web HTTP	unknown	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Unreachable (type=3 code=3)	UDP Port 1054	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 512	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 51100	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 135	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1981	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1434	Port Unreachable

Unreachable (type=3 code=3)	UDP Port 61466	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7000	Port Unreachable
Echo (type=0 code=0)	Echo Request	Echo Reply

■□□□□ 1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

172.17.1.1 (-, -)

Information Gathered (7)

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.1.1	No registered hostname

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 22, 443.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
4,6,8,10,12,14,16,22,26,28,30,34,36,40,224-227,230-234,236-239,241,247-248,
250-255,266-267,269-278,283-308,310,312-317,319-321,326-343,352-353,355-362,
364-368,443,582-586,588-591,594-597,599,601-605,621-622,625-626,628-630,
632,638-646,648-649,651-656,658-665,675-688,690-699,701-703,706,708,712,
714-723,725-727,732-739,743,745-746,755-757,766,768,779,784-785,787-793,
795-798,802-810,812-842,844-848,850-855,857-859,861-869,871-872,874-885,
889-894,896-899,903-910,913-922,925-931,933-949,951-953,956-989,994,1002-1007,
1009,1012-1014,1016-1022,1101-1103,1105-1108,1113,1115-1122,1124-1154,
1156-1160,1162-1166,1168-1169,1171-1182,1184-1186,1188, and more.
We have omitted from this list 59403 higher ports to keep the report size manageable.
```

■□□□□ 1 Host Scan Time

QID:	45038

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2169 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:12:48 GMT

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
UDP	67	0:00:17
UDP	123	0:00:19

▮▯▯▯▯ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
67	bootps	Bootstrap Protocol Server	unknown
123	ntp	Network Time Protocol	unknown

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 456	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 3636	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 445	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 27444	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 555	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 31337	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 69	Port Unreachable
Address Mask (type=18 code=0)	Address Mask Request	255.255.255.0
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable

1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

172.17.1.15 (host5.enterate.com, HOST5) Windows 2016

Vulnerabilities (1)

🟥🟥🟥□□ 3 Unauthenticated/Open Web Proxy Detected port 8014/tcp over SSL

QID:	62002
Category:	Proxy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/18/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Users with unauthorized internet access can connect to arbitrary services using the HTTP protocol via this proxy.

IMPACT:
Successful exploitation may allow unauthorized users to browse the Internet with your IP address , your Intranet and Web server. This may also be exploited to scan non-http services inside your firewall.

SOLUTION:
Reconfigure your proxy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
The Following Adressing Schemes Are Supported:
http://ip4_address
https://ip4_address
GET http://172.16.1.90:40453/ HTTP/1.0
```

Potential Vulnerabilities (4)

■■■■□ 4 Potential TCP Backdoor

QID:	1004
Category:	Backdoors and trojan horses
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/04/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

There are known backdoors that use specific port numbers. At least one of these ports was found open on this host. This may indicate the presence of a backdoor; however, it's also possible that this port is being used by a legitimate service, such as a Unix or Windows RPC.

IMPACT:

If a backdoor is present on your system, then unauthorized users can log in to your system undetected, execute unauthorized commands, and leave the host vulnerable to other unauthorized users. Malicious users may also use your host to access other hosts and perform a coordinated Denial of Service attack.
Some well-known backdoors are "BackOrifice", "Netbus" and "Netspy". You should be able to find more information on these backdoors on the CERT Coordination Center's Web site (www.cert.org) (http://www.cert.org).

SOLUTION:

Call a security specialist and test the host for backdoors. If a backdoor is found, then the host may need to be re-installed.

COMPLIANCE:

Type: CobIT
Section: DS5.9
Description: Malicious Software Prevention, Detection and Correction
Ensure that preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from Malware (viruses, worms, spyware, spam, internally developed fraudulent software, etc.).

Type: HIPAA
Section: 164.306 and 164.312
Description: Insuring that Malware is not present on hosts addresses section(s) 164.306 and 164.312 requirements for securing critical system files and services and insuring system integrity.

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The tcp port 5000 is open, it may indicate the presence of a "Socket23" backdoor.

■■■□□ 3 Apache Tomcat HTTP/2 Request Header Mix-Up Vulnerability

QID:	12375
Category:	CGI
CVE ID:	CVE-2020-17527
Vendor Reference:	Apache Tomcat 8.5.60, Apache Tomcat 9.0.40
Bugtraq ID:	-
Service Modified:	12/10/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
Affected by following vulnerability:
CVE-2020-17527 : Apache Tomcat could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream.
Affected Versions:
Apache Tomcat 8.5.0 to 8.5.59
Apache Tomcat 9.0.0-M1 to 9.0.39
QID Detection Logic (Unauthenticated):
The QID checks for vulnerable version by sending a GET /QUALYS13827 HTTP/1.0 request which helps in retrieving the installed version of Apache Tomcat in the banner of the response.

IMPACT:

Successful exploitation would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.

SOLUTION:

Upgrade to the Apache Tomcat 8.5.60, 9.0.40 or to the latest version of Apache Tomcat. Please refer to Apache Tomcat (http://tomcat.apache.org/index.html).
Workaround:- Disable support for the application/xml content type
- Apply security fix available in source code form (https://svn.apache.org/repos/asf/axis/axis2/java/core/security/secfix-cve-2010-1632) until a fixed version is available.
Detailed information on applying the workarounds can be found at Apache Axis advisory (https://svn.apache.org/repos/asf/axis/axis2/java/core/security/CVE-2010-1632.pdf).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Tomcat 8.5.60 (http://tomcat.apache.org/security-8.html)
Apache Tomcat 9.0.40 (http://tomcat.apache.org/security-9.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Apache Tomcat detected on port 8029.
<h3>Apache Tomcat/9.0.37</h3>Vulnerable version of Apache Tomcat detected on port 8015.

■■■□□ 3 OpenSSL Raccoon Attack Vulnerability(20200909)

QID:	38796
Category:	General remote services
CVE ID:	CVE-2020-1968
Vendor Reference:	20200909
Bugtraq ID:	-
Service Modified:	09/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSL is a commercial-grade, full-featured, open source toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, and provides a full-strength, general purpose cryptography library.
CVE-2020-1968: Vulnerability present in the TLS specification
Affected Versions:
OpenSSL 1.0.2-1.0.2v
QID Detection Logic:(Unauthenticated)
This QID matches vulnerable versions based on the exposed banner information.

IMPACT:

Successful exploitation allows an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite.

SOLUTION:

The vendor has released a patch. Fixed in OpenSSL 1.0.2w and 1.1.1 is not vulnerable. For more information please visit advisory (https://www.openssl.org/news/secadv/20200909.txt).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
20200909 (https://www.openssl.org/news/secadv/20200909.txt)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable OpenSSL version detected on port 8014 over TCP - Apache/2.4.41 (Win32) OpenSSL/1.0.2uVulnerable OpenSSL version detected on port 8015 over TCP -
Date: Sat, 20 Feb 2021 06:38:55 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0
Connection: close

■□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (110)

■■■□□ 3 Content-Security-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Content-Security-Policy HTTP Header missing on port 8014.
GET / HTTP/1.0
Host: host5.enterate.com:8014
```

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 8014/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8014.
GET / HTTP/1.0
Host: host5.enterate.com:8014

■■■□□ 3 Content-Security-Policy HTTP Security Header Not Detected port 8016/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8016.
GET / HTTP/1.0
Host: host5.enterate.com:8016

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 8016/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8016.
GET / HTTP/1.0
Host: host5.enterate.com:8016

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U6483:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

■■□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft

Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCOM System Activator	0.0	49705			
Microsoft Distributed Transaction Coordinator	1.0	50347			
Microsoft Local Security Architecture	0.0	49704, 49676			
Microsoft LSA DS Access	0.0	49704, 49676			
Microsoft Network Logon	1.0	49704, 49676			
Microsoft Scheduler Control Service	1.0	49705			
Microsoft Security Account Manager	1.0	49704, 49676			
Microsoft Task Scheduler	1.0	49705			
MS Wbem Transport IEnumWbemClassObject	0.0	49705			
MS Wbem Transport IWbemLevel1Login	0.0	49705			
MS Wbem Transport IWbemObjectSink	0.0	49705			
MS Wbem Transport IWbemServices	0.0	49705			
(Unknown Service)	1.0	49704, 49676			
(Unknown Service)	0.0	49705			
(Unknown Service)	1.0	49705			
(Unknown Service)	4.0	49705			
(Unknown Service)	2.0	49705			
(Unknown Service)	0.0	49704, 49676			
(Unknown Service)	2.0	49704, 49676			
(Unknown Service)	1.0	49664			

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 443, the host's uptime is 4 days, 13 hours, and 7 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

■■□□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8029/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8029 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8016/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 8016 port.GET / HTTP/1.1
```

■■□□□ 2 Web Server HTTP Protocol Versions port 8015/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 8015 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.1.15	host5.enterate.com

1 Microsoft SQL Server Instances Enumerated

QID:	19145
Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/24/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Microsoft SQL Server instances from the target Windows machine are enumerated.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Name: ARCSERVE_APP
 Port: 50053
 IsCluster: No
 Version: 12.0.5000.0
```

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2178,2180-2512,2514-2701,
2703-2868,2870-3342,3344-3388,3390-4999,5008-5630,5632-5984,5986-6049,
6051-6128,6130-6599,6601-7787,7789-7999,8001-8013,8017-8028,8030-8567,
8569-8957,8959-9679,9681-15001,15004-26999,27001-35896,35898-41522,41524-42423,
42425-47000,47002-49663,49665-49670,49672-49675,49677-49703,49706-49708,
49710-49715,49717-49736,49738-50062,50064-50346,50348-54529,54531-55157,
55159-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 3421 seconds

Start time: Sat, Feb 20 2021, 06:15:47 GMT

End time: Sat, Feb 20 2021, 07:12:48 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
host5.enterate.com	NTLM DNS
host5.enterate.com	FQDN
HOST5	MSSQL Monitor
HOST5	NTLM NetBIOS

1 Java Remote Method Invocation Detected

QID:	45186
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/23/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Java Remote Method Invocation or Java RMI, is a mechanism that allows one to invoke a method on an object that exists in another address space.
Java RMI is running on target host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Service name: Java RMI is running  on TCP port 9680.
Service name: Java RMI is running  on TCP port 8568.
```

1 OpenSSL (Open Source toolkit for SSL/TLS) Detected

QID:	45222

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/07/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSL is an open-source implementation of the SSL and TLS protocols. OpenSSL is based on SSLeay.
Qualys detected OpenSSL on the host. Please note that in remote detections, security patches may be backported and the displayed version number may not show the correct patch level.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
OpenSSL detected on port 8014 over TCP - Apache/2.4.41 (Win32) OpenSSL/1.0.2uOpenSSL detected on port 8015 over TCP -
Date: Sat, 20 Feb 2021 06:38:55 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0
Connection: close
```

■□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

▮▯▯▯▯ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45262 detected on port 445 over TCP.

SMBv2 is enabled.

1 Apache Tomcat Server Detected

QID:	45387
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Apache Tomcat
Bugtraq ID:	-
Service Modified:	07/06/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
QID Detection Logic (authenticated):
Operating System:Linux
The QID checks for running tomcat servers. The version is extracted from the catalina.jar using "unzip -p" command.
Note:unzip is needed for successful detection.

IMPACT:
NA

SOLUTION:
NA

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Apache Tomcat Server Detected on port: 8029
>Apache Tomcat/9.0.37</h3>Apache Tomcat Server Detected on port: 8015
```

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:07:16
TCP	443	0:03:57
TCP	445	0:00:01
TCP	2179	0:00:45
TCP	3343	0:07:10
TCP	3389	0:00:51
TCP	5000	0:02:09
TCP	5001	0:02:27
TCP	5002	0:02:09
TCP	5003	0:02:09
TCP	5004	0:02:09
TCP	5005	0:02:09
TCP	5006	0:02:24
TCP	5007	0:02:09
TCP	5985	0:27:37
TCP	6050	0:01:10
TCP	6600	0:02:52
TCP	7788	0:00:33
TCP	8000	0:01:54
TCP	8014	1:27:17
TCP	8015	1:16:43
TCP	8016	0:42:44
TCP	8029	0:40:44
TCP	8568	0:04:27
TCP	8958	0:04:14
TCP	9680	0:04:27
TCP	15002	0:06:34
TCP	15003	0:00:33
TCP	27000	0:02:08
TCP	41523	0:01:40
TCP	47001	0:27:39
TCP	49664	0:05:05
TCP	49671	0:05:05
TCP	49676	0:05:05
TCP	49704	0:05:05
TCP	49705	0:05:05
TCP	49709	0:05:05
TCP	49716	0:05:05
TCP	49737	0:05:05
TCP	50053	0:00:36
TCP	50063	0:01:51

TCP	50347	0:05:05
TCP	55158	0:02:47
UDP	1434	0:00:21

1 Java RMI Distributed Garbage-Collection Service Detected

QID:	48074
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Java RMI services can be exposed over network using TCP sockets. Every RMI service is identified by an object number.
Garbage-Collection Service (2 - DGC_ID) is detected on remote RMI service.
QID Detection Logic(Unauthenticated):
This QID sends a Java DGC RMI payload to the remote service.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Java RMI Distributed Garbage-Collection Service Detected on port 9680
Java RMI Distributed Garbage-Collection Service Detected on port 8568
```

1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Microsoft Server Message Block (SMBv3) Compression Disabled

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

▮▯▯▯▯ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
1434	ms-sql-m	Microsoft-SQL-Monitor	mssql monitor

1 Open TCP Services List

QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/15/2009
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	unknown	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
2179	vmrdp	Microsoft RDP for virtual machines	VMRDP	
3343	ms-cluster-net	MS Cluster Net	unknown	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5000	Socket23	backdoor commplex-main	unknown	
5001	commplex-link	commplex-link	unknown	

5002	rfe	radio free ethernet	unknown
5003	fmpro-internal	FileMaker, Inc. - Proprietary transport	unknown
5004	avt-profile-1	avt-profile-1	unknown
5005	avt-profile-2	avt-profile-2	unknown
5006	unknown	unknown	unknown
5007	unknown	unknown	unknown
5985	unknown	unknown	http
6050	x11	X Window System	unknown
6600	unknown	unknown	unknown
7788	unknown	unknown	unknown
8000	irdmi	iRDMI	unknown
8014	unknown	unknown	proxy http over ssl
8015	unknown	unknown	http over ssl
8016	unknown	unknown	http over ssl
8029	unknown	unknown	http over ssl
8568	unknown	unknown	RMIRegistry
8958	unknown	unknown	unknown
9680	unknown	unknown	RMIRegistry
15002	unknown	unknown	unknown
15003	unknown	unknown	unknown
27000	unknown	unknown	unknown
41523	unknown	unknown	unknown
47001	unknown	unknown	http
49664	unknown	unknown	msrpc
49671	unknown	unknown	msrpc
49676	unknown	unknown	msrpc
49704	unknown	unknown	msrpc
49705	unknown	unknown	msrpc
49709	unknown	unknown	msrpc
49716	unknown	unknown	msrpc
49737	unknown	unknown	msrpc
50063	unknown	unknown	unknown
50347	unknown	unknown	msrpc
55158	unknown	unknown	unknown

■□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)

IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	06:15:49 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HOST5

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1397862269 with a standard deviation of 602515965. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5106 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 3
Duration: 23 milli seconds
```

1 Apache Tomcat Web Server Running on Target

QID:	86990
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/03/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
Apache Tomcat is running on this target.
QID Detection Logic (Unauthenicated) :
The qid checks HTTP response header to identify the server name and also sends the GET request to non existing page (abc) and match the Tomcat string in response.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Apache Tomcat webserver running on this host on port: 8029
>Apache Tomcat/9.0.37</h3>Apache Tomcat webserver running on this host on port: 8015
```

1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8014.

```
GET / HTTP/1.0
Host: host5.enterate.com:8014



HTTP/1.1 200
Date: Sat, 20 Feb 2021 06:46:56 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Set-Cookie: AGENTJSESSIONID=5B9AACE4840BA486A6AFCDDE0E814842; Path=/; Secure; HttpOnly
Connection: close
```

1 Referrer-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8014 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8014/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubDomains

■□□□□ 1 HTTP Service Unavailable Replies Received port 8014/tcp

QID:	86383
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

We have received "503 Service Unavailable" replies in response to our HTTP requests. The server is temporarily unable to service your request due to maintenance downtime or capacity problems.

IMPACT:

The detection of possible Web Server vulnerabilities can be inconsistent as follows.

- Because our scanner could not access to this service,
there are possibility of missing some vulnerabilities which should be detected.

- If the target host is a Windows host, there is a possibility
that some
vulnerabilities for IIS that should be detected were not detected.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 503 Service Unavailable
Date: Sat, 20 Feb 2021 06:48:30 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Content-Length: 299
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>503 Service Unavailable</title>
</head><body>
<h1>Service Unavailable</h1>
<p>The server is temporarily unable to service your
request due to maintenance downtime or capacity
problems. Please try again later.</p>
</body></html>
```

■□□□□ 1 List of Web Directories port 8014/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
\	brute force
/css/	web page
/images/	web page
/images/default/	web page
/images/default/window/	web page

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:47001
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:31:19 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:31:23 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: host5.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:31:19 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 8014/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8014/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 SSL Server Information Retrieval port 8014/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8014/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8014/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8014/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	brainpoolp512r1	512	yes	256	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	brainpoolp384r1	384	yes	192	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low

ECDHE	secp256k1	256	yes	128	low
ECDHE	brainpoolp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 8014/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8014/tcp over SSL

QID:	38718
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8014/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8014/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	

countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84

(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8014/tcp over SSL

QID: 86565
Category: Web server

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.1.15:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.17.1.15:8014



HTTP/1.1 200
Date: Sat, 20 Feb 2021 06:59:11 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Set-Cookie: AGENTJSESSIONID=4958C067B6F815319D2B6D2488E6229B; Path=/; Secure; HttpOnly
Transfer-Encoding: chunked

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>

0

HTTP/1.1 404
Date: Sat, 20 Feb 2021 06:59:11 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html
Content-Length: 122

<html>
 <body >
  <div id="warning" style="width:100%;text-align:center;padding-top:20px;">404</div>
 </body >
</html>
```

▮□□□□ 1 HTTP Methods Returned by OPTIONS Request port 8029/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

1 HTTP Response Method and Header Information Collected port 8029/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 8029.

GET / HTTP/1.0
Host: host5.enterate.com:8029



HTTP/1.1 404
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 682
Date: Sat, 20 Feb 2021 06:38:42 GMT
Connection: keep-alive
Keep-Alive: timeout=20
```

1 List of Web Directories port 8029/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified: 09/10/2004
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/management/	brute force

■□□□□ 1 Default Web Page port 5985/tcp

QID: 12230
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:5985


HTTP/1.1 404 Not Found
```

```
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:33:43 GMT
Connection: close
Content-Length: 315

	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:33:58 GMT
Connection: close
Content-Length: 315

	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: host5.enterate.com:5985


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:33:43 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 8029/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:8029



<!doctype html><html lang="en"><head><title>HTTP Status 404  Not Found</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;}
h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;}
.line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 404  Not Found</h1><hr class="line" /><p><b>
Type</b> Status Report</p><p><b>Description</b> The origin server did not find a current representation for the target resource or is not willing to
disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.37</h3></body></html>
```

1 Default Web Page (Follow HTTP Redirection) port 8029/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:8029


<!doctype html><html lang="en"><head><title>HTTP Status 404  Not Found</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;}
h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;}
.line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 404  Not Found</h1><hr class="line" /><p><b>
Type</b> Status Report</p><p><b>Description</b> The origin server did not find a current representation for the target resource or is not willing to
disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.37</h3></body></html>
```

1 SSL Server Information Retrieval port 8029/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM

DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8029/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 8029/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8029/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

1 SSL/TLS Protocol Properties port 8029/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no

SCT extension	no

1 SSL Certificate Transparency Information port 8029/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8029/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8029/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1

(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13

(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

▮▯▯▯▯ 1 HTTP Methods Returned by OPTIONS Request port 8016/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

▮▯▯▯▯ 1 HTTP Response Method and Header Information Collected port 8016/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 8016.

```
GET / HTTP/1.0
Host: host5.enterate.com:8016



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=CA382605C6C68B1A4A90E14CF27FB2AA; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Date: Sat, 20 Feb 2021 06:42:55 GMT
Connection: close
```

▮□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 8016/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Referrer-Policy HTTP Header missing on 8016 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 8016/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubDomains

1 List of Web Directories port 8016/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/css/	web page
/images/	web page
/images/default/	web page
/images/default/window/	web page

1 Default Web Page port 8016/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:8016
```

```
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8016/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:8016



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 SSL Server Information Retrieval port 8016/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8016/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 8016/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8016/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

▮▯▯▯▯ 1 SSL/TLS Protocol Properties port 8016/tcp over SSL

QID: 38706
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

▮▯▯▯▯ 1 SSL Certificate Transparency Information port 8016/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control			

		Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63 a577e5be577d9c600af8f94d5d 265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1 f76d86e0232663adc04b7f5dc6 835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a09 42875e4e318b1b03ebeb4bc768 f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8016/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 8016/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95

(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)

(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8016/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.1.15:8016

GET /Q_Evasive/ HTTP/1.1
Host:172.17.1.15:8016
```

```
HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=E5C411923126CE3E1BC669931D2150E5; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 20 Feb 2021 06:59:09 GMT

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>

0

HTTP/1.1 404
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html
Content-Length: 122
Date: Sat, 20 Feb 2021 06:59:09 GMT

<html>
 <body >
  <div id="warning" style="width:100%;text-align:center;padding-top:20px;">404</div>
 </body >
</html>
```

1 HTTP Response Method and Header Information Collected port 8015/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 8015.

```
GET / HTTP/1.0
Host: host5.enterate.com:8015



HTTP/1.1 302
Date: Sat, 20 Feb 2021 06:52:47 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

■□□□□ 1 List of Web Directories port 8015/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/management/	brute force
\	brute force

1 Default Web Page port 8015/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:8015



HTTP/1.1 302
Date: Sat, 20 Feb 2021 06:52:47 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

1 Default Web Page (Follow HTTP Redirection) port 8015/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host5.enterate.com:8015



HTTP/1.1 302
Date: Sat, 20 Feb 2021 06:56:09 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: https://host5.enterate.com:8015/samlsso?SAMLRequest=nZNBj9owEIXv%2FRWW7yQhFZS1SFYUtCrStqWQ7aE34wxg1bFTz4Sl%
2F75OAi2HFqEeY8%2B89%2FzNZPp4qgw7gkftbMaHUcIZWOVKbfcZfymeBhP%2BmL%2BZoqxMLWYNHewafjSAxGaI4Cm0zZ3FpgK%2FAX%
2FUCl7WzxmPK2nlHiqwFCO62Li9trGSxmyl%2Bs7ZjMjrbUPQNwe3c%2FfSlnDKeDp69zAZj8acLYKXtpK6fAeiGkUc5ILUwSGJSTIcxW264MLZk%
2FMKupQZ30mDwNlykfHwqCWuJKI%2Bwp8LxCbYIUlLwTBJh4MkHaRJkYzFaCySh%2BjtJP3G2co7csqZ99r2VBpvhZOoUVhZAQpSYjP7%
2BCzSKBHbvgjFh6JYDVafNwVnXy9005Zu4G1RdDxvS9VnX56f6XeB%2Ff0C8jIgnitXRdKr8H2ECMo9RG3%
2FNL4W7m3SWnwKSsvFyhmtfrKZMe517kFSIEe%2BgQ5yJem2d3uiy8GuKxV1SwApLANnm1Wr%2F6WRRu80%
2BIz37tdg0nvJxL8zn5cSym74YakITsTmrqql19jCh5NU9F8uvYm4Vp6bAHcNuyu5u2dxs0wJ1UqH43ZdX50v2%2FUDFV5WeGmxdp76sf01T97f%
2FQtIfpn49Y%2Bc%2FwI%3D&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=Qm%
2FDacBwxVW3hoGc9VhAF2%2BC9UUDKYtpPWMwyEzMWV%2BiFrtzFOUqhybjwEVv5Xr90%
2FBHGfXGqqsRL7CIuv1RQyU2nVMgo6aZOmeFA3X9XEqDJzqnUTTNduc6FIvN4f45CAnAF3HSksZq%
2FjXNG0pHvV7qHrzF3kLIwBEfv12rx5M6MM7egdZvaurc31xp7Wp9T2HgXCSk1M3ZRhlYX3TBByPfmIu9o2HvqEaH7MGiFTSOeDz1XkMe7fFTLFy-
ka1ea6BOfg4xbTWK6tuB6NbSU86Z%2FBMtHqQMY1w5LLpFcOZnnKgTvAVnOUo2reVlq5Y8QdpZLzYu98FKc3Z2wtjuoVQ%3D%3D
Content-Length: 0
Set-Cookie: isDBAvailable=checked
Set-Cookie: EDGEJSESSIONID=CB8FCAFD679221A420926E73285C0078; Path=/management; Secure; HttpOnly
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

▮▯▯▯▯ 1 SSL Server Information Retrieval port 8015/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8015/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8015/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303

0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8015/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	brainpoolp512r1	512	yes	256	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	brainpoolp384r1	384	yes	192	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low
ECDHE	brainpoolp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 8015/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 8015/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8015/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8015/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT

(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)

(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8015/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.1.15:8015

GET /Q_Evasive/ HTTP/1.1
Host:172.17.1.15:8015



HTTP/1.1 302
Date: Sat, 20 Feb 2021 06:59:40 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Location: /management/
Content-Length: 0

HTTP/1.1 404
Date: Sat, 20 Feb 2021 06:59:40 GMT
Server: Apache/2.4.41 (Win32) OpenSSL/1.0.2u
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 682

<!doctype html><html lang="en"><head><title>HTTP Status 404 _E2_80_93 Not Found</title><style type="text/css">body {font-family:Tahoma,Arial,
sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a
{color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 404 _E2_80_93 Not Found</h1><
hr class="line" /><p><b>Type</b> Status Report</p><p><b>Description</b> The origin server did not find a current representation for the target
resource or is not willing to disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.37</h3></body></html>
```

1 Microsoft SQL Server Cluster Presence Check port 1434/udp

QID:	19101
Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/30/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner probed the target Microsoft SQL Server to determine if a cluster is being used. Using SQL clustering is required for redundancy/fail-over purposes. The results of the check are posted below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SQL Cluster Not Installed

■□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH

ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low

ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:

(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:

(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.1.16 (host6.enterate.com, HOST6) Windows 2016

Potential Vulnerabilities (1)

■□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (55)

■■■□□ 3 Content-Security-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy

Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Content-Security-Policy HTTP Header missing on port 8014.
GET / HTTP/1.0
Host: host6.enterate.com:8014
```

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 8014/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 8014.
GET / HTTP/1.0
Host: host6.enterate.com:8014
```

▮▮□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U6483:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

▮▮▯▯▯ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCOM System Activator	0.0	49702			
Microsoft Distributed Transaction Coordinator	1.0	49857			
Microsoft Local Security Architecture	0.0	49713, 49675			
Microsoft LSA DS Access	0.0	49713, 49675			
Microsoft Network Logon	1.0	49713, 49675			
Microsoft Scheduler Control Service	1.0	49702			
Microsoft Security Account Manager	1.0	49713, 49675			
Microsoft Task Scheduler	1.0	49702			
MS Wbem Transport IEnumWbemClassObject	0.0	49702			
MS Wbem Transport IWbemLevel1Login	0.0	49702			
MS Wbem Transport IWbemObjectSink	0.0	49702			
MS Wbem Transport IWbemServices	0.0	49702			
(Unknown Service)	1.0	49713, 49675			
(Unknown Service)	0.0	49702			
(Unknown Service)	1.0	49702			
(Unknown Service)	4.0	49702			
(Unknown Service)	2.0	49702			
(Unknown Service)	1.0	49668			
(Unknown Service)	0.0	49713, 49675			
(Unknown Service)	2.0	49713, 49675			

■■□□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Based on TCP timestamps obtained via port 443, the host's uptime is 4 days, 7 hours, and 16 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.
```

■■□□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.1.16	host6.enterate.com

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2178,2180-2512,2514-2701,
2703-3342,3344-3388,3390-5630,5632-5984,5986-6128,6130-6599,6601-8013,
8015-26999,27001-42423,42425-47000,47002-49667,49670-49674,49676-49701,
49704-49707,49709-49712,49714-49722,49724-49856,49858-65535

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2356 seconds

Start time: Sat, Feb 20 2021, 06:15:28 GMT

End time: Sat, Feb 20 2021, 06:54:44 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
host6.enterate.com	NTLM DNS
host6.enterate.com	FQDN
HOST6	NTLM NetBIOS

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:07:29
TCP	443	0:03:57
TCP	445	0:00:01
TCP	2179	0:00:45
TCP	3343	0:07:10
TCP	3389	0:00:51
TCP	5985	0:27:37
TCP	6600	0:02:42
TCP	8014	0:52:27
TCP	27000	0:03:52
TCP	47001	0:27:38
TCP	49668	0:05:07
TCP	49669	0:05:05
TCP	49675	0:05:05
TCP	49702	0:05:05
TCP	49703	0:05:05
TCP	49708	0:05:05
TCP	49713	0:05:05
TCP	49723	0:05:10
TCP	49857	0:05:05

▮□□□□ 1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Microsoft Server Message Block (SMBv3) Compression Disabled

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	unknown	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
2179	vmrdp	Microsoft RDP for virtual machines	VMRDP	
3343	ms-cluster-net	MS Cluster Net	unknown	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
6600	unknown	unknown	unknown	
8014	unknown	unknown	http over ssl	
27000	unknown	unknown	unknown	
47001	unknown	unknown	http	
49668	unknown	unknown	msrpc	
49669	unknown	unknown	msrpc	
49675	unknown	unknown	msrpc	
49702	unknown	unknown	msrpc	
49703	unknown	unknown	msrpc	
49708	unknown	unknown	msrpc	
49713	unknown	unknown	msrpc	
49723	unknown	unknown	msrpc	
49857	unknown	unknown	msrpc	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	06:15:30 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HOST6

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 960360951 with a standard deviation of 638868389. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5107 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2
Duration: 22 milli seconds
```

1 HTTP Methods Returned by OPTIONS Request port 8014/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8014.

```
GET / HTTP/1.0
Host: host6.enterate.com:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=585A4C0DBD7B8E34CE338462BE00C0B2; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Date: Sat, 20 Feb 2021 06:24:18 GMT
Connection: close
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8014 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8014/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubDomains

1 List of Web Directories port 8014/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/css/	web page
/images/	web page
/images/default/	web page
/images/default/window/	web page

1 Default Web Page port 8014/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host6.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8014/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host6.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

1 SSL Server Information Retrieval port 8014/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8014/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes

only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8014/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8014/tcp over SSL

QID:	38704
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

1 SSL/TLS Protocol Properties port 8014/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8014/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8014/tcp over SSL

QID: 42350
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 8014/tcp over SSL

QID: 86002
Category: Web server
CVE ID: -
Vendor Reference: -

Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:

(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT

(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8014/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.1.16:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.17.1.16:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=FE8FAB62EE609625AECEC8075B8825CB; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 20 Feb 2021 06:52:34 GMT

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>

0

HTTP/1.1 404
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 0
Date: Sat, 20 Feb 2021 06:52:34 GMT
```

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host6.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:26:17 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host6.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:26:30 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: host6.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:26:17 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host6.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:29:24 GMT
Connection: close
Content-Length: 315

   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
```

```
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host6.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:29:34 GMT
Connection: close
Content-Length: 315

   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: host6.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:29:24 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

■□□□□ 1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

▮□□□□ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1

(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13

(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:

(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.1.17 (host7.enterate.com, HOST7) Windows 2016

Potential Vulnerabilities (2)

■■■□□ 3 Apache Tomcat HTTP/2 Request Header Mix-Up Vulnerability

QID:	12375
Category:	CGI
CVE ID:	CVE-2020-17527
Vendor Reference:	Apache Tomcat 8.5.60, Apache Tomcat 9.0.40
Bugtraq ID:	-
Service Modified:	12/10/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
Affected by following vulnerability:
CVE-2020-17527 : Apache Tomcat could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream.
Affected Versions:
Apache Tomcat 8.5.0 to 8.5.59
Apache Tomcat 9.0.0-M1 to 9.0.39
QID Detection Logic (Unauthenticated):
The QID checks for vulnerable version by sending a GET /QUALYS13827 HTTP/1.0 request which helps in retrieving the installed version of Apache Tomcat in the banner of the response.

IMPACT:

Successful exploitation would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests.

SOLUTION:

Upgrade to the Apache Tomcat 8.5.60, 9.0.40 or to the latest version of Apache Tomcat. Please refer to Apache Tomcat (http://tomcat.apache.org/

index.html).
Workaround:- Disable support for the application/xml content type
- Apply security fix available in source code form (https://svn.apache.org/repos/asf/axis/axis2/java/core/security/secfix-cve-2010-1632) until a fixed version is available.
Detailed information on applying the workarounds can be found at Apache Axis advisory (https://svn.apache.org/repos/asf/axis/axis2/java/core/security/CVE-2010-1632.pdf).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Tomcat 8.5.60 (http://tomcat.apache.org/security-8.html)
Apache Tomcat 9.0.40 (http://tomcat.apache.org/security-9.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable version of Apache Tomcat detected on port 8020.
<h3>Apache Tomcat/9.0.38</h3>

■□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Service name: Unknown - Possible Scan Interference on TCP port 443.

Information Gathered (77)

3 Content-Security-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Content-Security-Policy HTTP Header missing on port 8014.
GET / HTTP/1.0
Host: host7.enterate.com:8014
```

3 HTTP Public-Key-Pins Security Header Not Detected port 8014/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8014.
GET / HTTP/1.0
Host: host7.enterate.com:8014

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U6483:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCOM System Activator	0.0	49700			
Microsoft Distributed Transaction Coordinator	1.0	49992			
Microsoft Local Security Architecture	0.0	49674, 49699			
Microsoft LSA DS Access	0.0	49674, 49699			
Microsoft Network Logon	1.0	49674, 49699			
Microsoft Scheduler Control Service	1.0	49700			
Microsoft Security Account Manager	1.0	49674, 49699			
Microsoft Task Scheduler	1.0	49700			
MS Wbem Transport IEnumWbemClassObject	0.0	49700			
MS Wbem Transport IWbemLevel1Login	0.0	49700			

MS Wbem Transport IWbemObjectSink	0.0	49700
MS Wbem Transport IWbemServices	0.0	49700
(Unknown Service)	1.0	49674, 49699
(Unknown Service)	0.0	49700
(Unknown Service)	1.0	49700
(Unknown Service)	0.0	49674, 49699
(Unknown Service)	2.0	49674, 49699
(Unknown Service)	4.0	49700
(Unknown Service)	2.0	49700
(Unknown Service)	1.0	49668

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 443, the host's uptime is 4 days, 6 hours, and 31 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Access to Remote Registry Service is denied, error: 0x0

2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8020/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 8020 port.GET / HTTP/1.1
```

■■□□□ 2 Web Server HTTP Protocol Versions port 6054/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 6054 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.1.17	host7.enterate.com

1 Microsoft SQL Server Instances Enumerated

QID:	19145
Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/24/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Microsoft SQL Server instances from the target Windows machine are enumerated.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Name: ARCSERVE_DB
 Port: 55309
 IsCluster: No
 Version: 12.0.5000.0
```

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2178,2180-2512,2514-2701,
```

2703-3342,3344-3388,3390-5630,5632-5984,5986-6049,6051,6053,6055-6128,
6130-6501,6505-6599,6601-8013,8015-8019,8021-10275,10277-41522,41524-42423,
42425-47000,47002-49667,49670-49673,49675-49698,49701-49702,49704-49720,
49722-49723,49725-49728,49730-49738,49740-49743,49745-49794,49796-49808,
49810-49830,49832-49991,49993-64277,64279-65535

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2588 seconds

Start time: Sat, Feb 20 2021, 05:41:42 GMT

End time: Sat, Feb 20 2021, 06:24:50 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
host7.enterate.com	NTLM DNS
host7.enterate.com	FQDN
HOST7	MSSQL Monitor
HOST7	NTLM NetBIOS

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

■□□□□ 1 Apache Tomcat Server Detected

QID:	45387
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Apache Tomcat
Bugtraq ID:	-

Service Modified:	07/06/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
QID Detection Logic (authenticated):
Operating System:Linux
The QID checks for running tomcat servers. The version is extracted from the catalina.jar using "unzip -p" command.
Note:unzip is needed for successful detection.

IMPACT:
NA

SOLUTION:
NA

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Apache Tomcat Server Detected on port: 8020
>Apache Tomcat/9.0.38</h3>
```

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:08:07
TCP	443	0:03:57
TCP	445	0:00:01
TCP	2179	0:00:45
TCP	3343	0:07:11
TCP	3389	0:00:51
TCP	5985	0:29:13
TCP	6050	0:01:12
TCP	6052	0:01:54
TCP	6054	0:28:07
TCP	6502	0:13:02
TCP	6503	0:11:32
TCP	6504	0:11:32
TCP	6600	0:02:42
TCP	8014	0:54:42
TCP	8020	0:45:06
TCP	41523	0:01:38
TCP	47001	0:27:37
TCP	49668	0:05:06
TCP	49669	0:05:05
TCP	49674	0:05:05
TCP	49699	0:05:05
TCP	49700	0:05:10
TCP	49703	0:05:21
TCP	49721	0:10:26
TCP	49724	0:10:26
TCP	49729	0:05:09
TCP	49739	0:10:27
TCP	49744	0:10:26
TCP	49795	0:05:05
TCP	49809	0:10:28
TCP	49831	0:10:38
TCP	49992	0:05:10
TCP	55309	0:00:36
UDP	111	0:00:07
UDP	1434	0:00:21

1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Microsoft Server Message Block (SMBv3) Compression Disabled

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session

Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most

(but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
111	sunrpc	SUN Remote Procedure Call	rpc udp
1434	ms-sql-m	Microsoft-SQL-Monitor	mssql monitor

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port

135	msrpc-epmap	epmap DCE endpoint resolution	unknown
443	https	http protocol over TLS/SSL	unknown
445	microsoft-ds	Microsoft-DS	microsoft-ds
2179	vmrdp	Microsoft RDP for virtual machines	VMRDP
3343	ms-cluster-net	MS Cluster Net	unknown
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl
5985	unknown	unknown	http
6050	x11	X Window System	unknown
6052	x11	X Window System	unknown
6054	unknown	unknown	http
6502	boks servm	BoKS Servm	unknown
6503	boks clntd	BoKS Clntd	unknown
6504	unknown	unknown	unknown
6600	unknown	unknown	unknown
8014	unknown	unknown	http over ssl
8020	unknown	unknown	http over ssl
41523	unknown	unknown	unknown
47001	unknown	unknown	http
49668	unknown	unknown	msrpc
49669	unknown	unknown	msrpc
49674	unknown	unknown	msrpc
49699	unknown	unknown	msrpc
49700	unknown	unknown	msrpc
49703	unknown	unknown	msrpc
49721	unknown	unknown	rpc
49724	unknown	unknown	rpc
49729	unknown	unknown	msrpc
49739	unknown	unknown	rpc
49744	unknown	unknown	rpc
49795	unknown	unknown	msrpc
49809	unknown	unknown	rpc
49831	unknown	unknown	rpc
49992	unknown	unknown	msrpc

■□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:41:44 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HOST7

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1178711480 with a standard deviation of 647923711. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5107 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2
Duration: 27 milli seconds

1 Apache Tomcat Web Server Running on Target

QID:	86990
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/03/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
Apache Tomcat is running on this target.
QID Detection Logic (Unauthenicated) :
The qid checks HTTP response header to identify the server name and also sends the GET request to non existing page (abc) and match the Tomcat string in response.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Apache Tomcat webserver running on this host on port: 8020
>Apache Tomcat/9.0.38</h3>
```

1 HTTP Methods Returned by OPTIONS Request port 8014/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS

■□□□□ 1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 8014.

```
GET / HTTP/1.0
Host: host7.enterate.com:8014


HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=673E336AE84E11D36EE7D03206AF1F08; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528738226000"
Last-Modified: Mon, 11 Jun 2018 17:30:26 GMT
Content-Type: text/html;charset=utf-8
```

Date: Sat, 20 Feb 2021 05:48:19 GMT
Connection: close

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8014 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8014/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubDomains

■□□□□ 1 List of Web Directories port 8014/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/css/	web page
/images/	web page
/images/default/	web page
/images/default/window/	web page

■□□□□ 1 Default Web Page port 8014/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
```

```
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 8014/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 SSL Server Information Retrieval port 8014/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH

ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8014/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 8014/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the

target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8014/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

ECDHE	secp521r1	521	yes	260	low

1 SSL/TLS Protocol Properties port 8014/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8014/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8014/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS

connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8014/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US

stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT

(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8014/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.1.17:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.17.1.17:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=1A0E48AD5F34A31111456C05BB4C9014; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528738226000"
Last-Modified: Mon, 11 Jun 2018 17:30:26 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 20 Feb 2021 06:18:31 GMT

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
```

```
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>

0

HTTP/1.1 404
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 0
Date: Sat, 20 Feb 2021 06:18:31 GMT
```

1 Default Web Page port 8020/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:8020


<!doctype html><html lang="en"><head><title>HTTP Status 404  Not Found</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;}
h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;}
.line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 404  Not Found</h1><hr class="line" /><p><b>
```

```
Type</b> Status Report</p><p><b>Message</b> The requested resource [/] is not available</p><p><b>Description</b> The origin server did not
find a current representation for the target resource or is not willing to disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.38</
h3></body></html>
```

1 Default Web Page (Follow HTTP Redirection) port 8020/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:8020


<!doctype html><html lang="en"><head><title>HTTP Status 404  Not Found</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;}
h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;}
.line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 404  Not Found</h1><hr class="line" /><p><b>
Type</b> Status Report</p><p><b>Message</b> The requested resource [/] is not available</p><p><b>Description</b> The origin server did not
find a current representation for the target resource or is not willing to disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/9.0.38</
h3></body></html>
```

1 SSL Server Information Retrieval port 8020/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8020/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8020/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303

0499	0303

▮□□□□ 1 SSL/TLS Key Exchange Methods port 8020/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low

▮□□□□ 1 SSL/TLS Protocol Properties port 8020/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8020/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to

allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8020/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

▮▯▯▯▯ 1 SSL Certificate - Information port 8020/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption

(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02

(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 8020/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 8020/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 8020.

GET / HTTP/1.0
Host: host7.enterate.com:8020


HTTP/1.1 404
Content-Type: text/html;charset=utf-8
Content-Language: en
```

```
Content-Length: 751
Date: Sat, 20 Feb 2021 05:56:15 GMT
Connection: keep-alive
Keep-Alive: timeout=60
```

1 Default Web Page port 6054/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:6054



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:01:49 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 6054/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:6054



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:02:37 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

▮□□□□ 1 HTTP Response Method and Header Information Collected port 6054/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 6054.

```
GET / HTTP/1.0
Host: host7.enterate.com:6054



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:01:49 GMT
Connection: close
Content-Length: 315
```

1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
```

```
Host: host7.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:06:13 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:06:20 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
```

```
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: host7.enterate.com:5985


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:06:13 GMT
Connection: close
Content-Length: 315
```

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:08:16 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: host7.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:09:34 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: host7.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:08:16 GMT
Connection: close
Content-Length: 315
```

▮□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH

AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server

OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

▮□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:

(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:

(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)

(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

■□□□□ 1 Microsoft SQL Server Cluster Presence Check port 1434/udp

QID: 19101

Category:	Database
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/30/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner probed the target Microsoft SQL Server to determine if a cluster is being used. Using SQL clustering is required for redundancy/fail-over purposes. The results of the check are posted below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SQL Cluster Not Installed

172.17.1.80 (util17-4.enterate.com, UTIL17-4) Windows 2012 R2 Standard

Information Gathered (35)

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2012 R2 Standard	CIFS via TCP Port 445	
Windows 2012 R2/8.1	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U6483:135

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Message Queuing - QM2QM V1	1.0	2107, 2103, 2105, 49175			
Message Queuing - QMRT V1	1.0	2107, 2103, 2105, 49175			
Message Queuing - QMRT V2	1.0	2107, 2103, 2105, 49175			
Message Queuing - RemoteRead V1	1.0	2107, 2103, 2105, 49175			

Microsoft Local Security Architecture	0.0	49171, 49155
Microsoft LSA DS Access	0.0	49171, 49155
Microsoft Network Logon	1.0	49171, 49155
Microsoft Scheduler Control Service	1.0	49154
Microsoft Security Account Manager	1.0	49171, 49155
Microsoft Server Service	3.0	49154
Microsoft Task Scheduler	1.0	49154
MS Wbem Transport IEnumWbemClassObject	0.0	49154
MS Wbem Transport IWbemLevel1Login	0.0	49154
MS Wbem Transport IWbemObjectSink	0.0	49154
MS Wbem Transport IWbemServices	0.0	49154
(Unknown Service)	1.0	49171, 49155
(Unknown Service)	0.0	2107, 2103, 2105, 49154, 49175
(Unknown Service)	0.0	49154
(Unknown Service)	1.0	2107, 2103, 2105, 49175
(Unknown Service)	1.0	49154
(Unknown Service)	1.0	49152
(Unknown Service)	0.0	49171, 49155
(Unknown Service)	4.0	49154

▮▮▯▯▯ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 445, the host's uptime is 8 days, 21 hours, and 28 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Access to Remote Registry Service is denied, error: 0x0
```

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.1.80	util17-4.enterate.com

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 443, 1.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-444,446-1705,1707-1800,1802-1999,2001-2102,2104,2106,2108-2146,
2148-2512,2514-2701,2703-2868,2870-3388,3390-5630,5632-5984,5986-6128,
6130-42423,42425-47000,47002-49151,49156-49170,49172-49174,49176-49180,
49182,49184-65535
```

■□□□□ 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2393 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:16:32 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
util17-4.enterate.com	NTLM DNS
util17-4.enterate.com	FQDN
UTIL17-4	NTLM NetBIOS

■□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:08:24
TCP	445	0:01:07
TCP	3389	0:00:52
TCP	5985	0:31:41
TCP	47001	0:33:11
TCP	49152	0:05:05
TCP	49153	0:05:05
TCP	49154	0:05:23
TCP	49155	0:05:05
TCP	49171	0:05:05
TCP	49175	0:05:05
TCP	49181	0:05:05
TCP	49183	0:05:05

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1801	msmq	Microsoft Message Que	Microsoft Message Queue Server	
2103	zephyr-clt	Zephyr serv-hm connection	msrpc	
2105	minipay	MiniPay	msrpc	
2107	unknown	unknown	msrpc	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
47001	unknown	unknown	http	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	
49155	unknown	unknown	msrpc	
49171	unknown	unknown	msrpc	
49175	unknown	unknown	msrpc	
49181	unknown	unknown	msrpc	
49183	unknown	unknown	msrpc	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:36:41 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

UTIL17-4

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1017658836 with a standard deviation of 617758141. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5100 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 25 milli seconds
```

1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-4.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:01 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-4.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:04 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: util17-4.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:01 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-4.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:54:44 GMT
Connection: close
Content-Length: 315

	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-4.enterate.com:47001
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:54:48 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: util17-4.enterate.com:47001


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:54:44 GMT
Connection: close
Content-Length: 315
```

▮□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮□□□□ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			

Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95

(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)

(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:

(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.1.253 (sfr17-1.enterate.com, -)

Information Gathered (5)

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.1.253	sfr17-1.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,
2102-2146,2148-2512,2514-2701,2703-2868,2870-3388,3390-5491,5493-5504,
5506-5549,5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,
6130-7006,7008-7009,7011-8304,8306-9098,9100-9989,9991-10109,10111-15580,
15582-42423,42425-51970,51972-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2487 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:18:34 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
sfr17-1.enterate.com	FQDN

■□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

172.17.1.254 (asa17-1.enterate.com, -) CheckPoint FW1

Vulnerabilities (3)

🟥🟥□□□ 2 SSL Certificate - Self-Signed Certificate port 443/tcp over SSL

QID:	38169
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/23/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
The client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.
By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 unstructuredName=asa17-1.enterate.com,CN=asa17-1.enterate.com is a self signed certificate.

🟥🟥□□□ 2 SSL Certificate - Signature Verification Failed Vulnerability port 443/tcp over SSL

QID:	38173
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/25/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 unstructuredName=asa17-1.enterate.com,CN=asa17-1.enterate.com self signed certificate

🟥🟥□□□ 2 SSL Certificate - Invalid Maximum Validity Date Detected port 443/tcp over SSL

QID:	38685
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/25/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Starting 1 March 2018, Certification Authorities (CAs) are not permitted to issue SSL certificates (issued from a public root) with a validity period greater than 27 months.

SSL/TLS certificate maximum validity is 825 days (27 months) for Domain Validated (DV) and Organization Validated (OV) Certificates.
SSL certificates have limited validity periods so that the certificate's holder identity information is re-authenticated more frequently.
It is detected that maximum validity of certificate on the system is more than what is recommended.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate with recommended maximum validity.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 unstructuredName=asa17-1.enterate.com,CN=asa17-1.enterate.com is valid for more than 825 days

Potential Vulnerabilities (1)

■□□□□ 1 Possible Scan Interference

QID:	42432
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/09/2021
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Possible scan interference detected.
A PCI scan must be allowed to perform scanning without interference from intrusion detection systems or intrusion prevention systems.
The PCI ASV is required to post fail if scan interference is detected.
The goal of this QID is to ensure that Active Protection Systems are not blocking, filtering, dropping or modifying network packets from a PCI Certified Scan, as such behavior could affect an ASV's ability to detect vulnerabilities. Active Protection Systems could include any of the following; IPS, WAF, Firewall, NGF, QoS Device, Spam Filter, etc. which are dynamically modifying their behavior based on info gathered from traffic patterns.
This QID is triggered if a well known and popular service is not identified correctly due to possible scan interference. Services like FTP, SSH, Telnet, DNS, HTTP and Database services like MSSQL, Oracle, MySql are included.
-If an Active Protection System is found to be preventing the scan from completing, Merchants should make the required changes (e.g. whitelist) so that the ASV scan can complete unimpeded.
-If the scan was not actively blocked, Merchants can submit a PCI False Positive/Exception Request with a statement asserting that No Active Protection System is present or blocking the scan.
Additionally, if there is no risk to the Cardholder Data Environment, such as no web service running, this can also be submitted as a PCI False Positive/Exception Request and reviewed per the standard PCI Workflow.
For more details on scan interference during a PCI scan please refer to ASV Scan Interference section of PCI DSS Approved Scanning Vendors Program Guide Version 3.1 July 2018 (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1611566661151).

IMPACT:

If the scanner cannot detect vulnerabilities on Internet-facing systems because the scan is blocked by an IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

SOLUTION:

Whitelist the Qualys scanner to scan without interference from the IDS or IPS.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: Unknown - Possible Scan Interference on TCP port 22.

Information Gathered (20)

■■■□□ 3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/23/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: SNMP on UDP port 161.

■■□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
CheckPoint FW1	TCP/IP Fingerprint	U4050:22

■■□□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 443, the host's uptime is 7 days, 13 hours, and 50 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.1.254	asa17-1.enterate.com

▮▯▯▯▯ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 23, 25, 53, 80, 111, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-21,23-442,444-2868,2870-6128,6130-32971,32973-65535

■□□□□ 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2320 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:15:47 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
asa17-1.enterate.com	FQDN

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	22	0:00:50

TCP	443	0:02:46
UDP	161	0:03:12

▮▯▯▯▯ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
161	snmp	SNMP	snmp

▮▯▯▯▯ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	unknown	
443	https	http protocol over TLS/SSL	socks5 over ssl	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 903250723 with a standard deviation of 622959562. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5114 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 22: 176 1374 1858 2533 2953 4004 4531 4882 6045 6195 6791 7333 7665 8864 9904 10671 10989 12117 12790 14631 17156 17501 18738 19458 21611 23116 24466 26115 27282
Duration: 27 milli seconds

■□□□□ 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM

AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		1024	yes	80	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID: 38706
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no

Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: not supported.

■□□□□ 1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	1168602459 (0x45a7755b)
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
commonName	asa17-1.enterate.com
unstructuredName	asa17-1.enterate.com
(0)SUBJECT NAME	
commonName	asa17-1.enterate.com
unstructuredName	asa17-1.enterate.com
(0)Valid From	Jan 27 16:23:48 2019 GMT
(0)Valid Till	Jan 24 16:23:48 2029 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:8b:2c:b7:b0:f3:36:7d:bc:1b:56:87:1d:97:c6:
(0)	80:4c:6a:eb:b1:68:c5:ce:ac:0f:86:d0:0f:80:5a:
(0)	b2:b1:3c:7c:4f:68:7c:ad:52:56:80:44:ff:6b:46:
(0)	50:54:5e:67:62:95:ef:8c:f8:68:73:d1:eb:69:6e:
(0)	e5:60:21:ed:08:13:1e:7b:76:c6:93:76:94:97:8c:
(0)	25:d5:0e:05:2e:59:0f:bc:75:64:12:2a:f1:6a:10:
(0)	f8:12:e5:c7:10:d9:df:45:92:e0:d3:db:65:a4:1b:
(0)	9a:8f:a7:48:72:4d:61:68:b7:25:1d:c9:f2:e2:03:
(0)	b0:24:c9:c1:13:cf:71:09:63:fc:1e:6f:a5:f2:86:
(0)	00:a7:49:af:a3:b5:7c:95:cd:72:9b:65:f4:60:83:
(0)	e7:f1:9d:16:20:90:17:87:e5:bb:84:de:aa:8e:2d:
(0)	6e:a8:c6:af:67:fd:77:ef:89:1d:54:47:96:4f:10:
(0)	4c:9a:a1:cb:e9:11:26:9c:8c:4d:cf:e7:bf:a0:c3:
(0)	06:24:82:21:23:b8:45:17:78:19:44:87:e5:20:9e:
(0)	47:5e:60:06:68:09:c1:93:b4:d9:1f:9e:e5:88:5a:
(0)	47:0d:39:c7:25:fd:20:fd:69:c6:aa:9e:26:a4:bb:
(0)	4a:85:58:0a:00:e3:5e:d1:b0:03:10:1b:4f:7d:7f:
(0)	ad:67
(0)	Exponent: 65537 (0x10001)
(0)Signature	(256 octets)
(0)	09:f7:10:f2:5e:f8:ae:b6:3b:f4:c2:c1:dd:db:dc:75
(0)	32:30:04:d1:7e:4c:43:8d:bb:22:3d:98:41:f4:dd:b2
(0)	61:58:1d:e8:04:ae:08:3b:a0:79:27:e7:34:38:8d:5a

(0)	72:fd:a0:f6:49:48:d8:d0:e3:56:74:1b:2d:81:70:af
(0)	4f:8e:11:69:49:fa:ef:0a:80:83:1b:c4:bf:68:3c:b3
(0)	e5:6e:32:7d:f0:43:bc:a7:df:74:46:cc:56:61:21:bc
(0)	cf:f4:40:ff:eb:ff:07:fc:03:45:83:b9:a2:87:2f:c3
(0)	15:9d:39:c8:e3:e4:19:aa:a9:fd:9c:c4:3f:c0:1e:83
(0)	28:61:98:7f:4e:fa:ec:48:81:7a:8e:ef:68:d7:6d:29
(0)	69:df:c8:8e:c9:4a:ba:4f:74:6c:f3:b1:07:cb:5f:45
(0)	01:b3:71:be:61:ab:b9:ae:be:d4:d3:d3:0d:de:5c:dc
(0)	d8:78:79:24:10:f5:f0:53:60:da:a7:21:a1:b0:e6:b9
(0)	b5:b8:e1:0c:15:ec:0e:2b:9f:65:e8:90:89:b1:0e:5c
(0)	63:a5:de:c6:0d:9a:3e:5c:2a:0e:3b:d0:fd:e3:43:7f
(0)	51:24:33:a8:0d:43:5b:f7:dd:4e:9e:4d:c2:2f:94:96
(0)	28:a9:d0:6b:82:91:0d:1f:67:5d:14:c6:e9:47:09:08

172.17.10.5 (dc2.enterate.com, DC2) Windows 2016

Potential Vulnerabilities (1)

■■□□□ 2 DNS Server Allows Remote Clients to Snoop the DNS Cache port 53/udp

QID:	15035
Category:	DNS and BIND
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/13/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The DNS server was found to allow DNS cache snooping. This means, any attacker could remotely check if a given domain name is cached on the DNS server.
This issue occurs when a target DNS server allows an untrusted client to make non-recursive DNS queries for domains that the target DNS server is not authoritative on. If the target DNS server consults its cache and replies with a valid answer (the IP address or "does not exist" NXDOMAIN reply), it is vulnerable to this attack. This tells the attacker that someone from the target network recently resolved that particular domain name.
QID Detection Logic (unauthenticated):
We make a DNS A query for testdeadenddummy.qualys.com from the target DNS server. The Recursive Query flag is set in this query. This means that the target DNS server will recursively search for the address of testdeadenddummy.qualys.com domain name and reply with an IP address to our scanner. If we do not get a reply we quit without posting a vuln.
- Next, we make the same DNS "A" query for the same domain-name name testdeadenddummy.qualys.com. However, this time we leave the "Recursive Query" flag unset. This means, we are requesting the target DNS server to check its cache or pre-defined DNS zone information for the IP address of the testdeadenddummy.qualys.com domain name. (If no information is present there, it should not find this information recursively from other DNS servers, and should simply reply with a non-found message). Since no other DNS server will have a zone for qualys.com, if we do get a reply, it has to be from the cache. If we do not get a response, we quit.
- If we do get a valid IP address in the reply, it means the DNS server consulted its cache and replied with the IP address of a site it recently cached. So an attacker can see what sites are cached in the DNS server by making non-recursive "A" requests for them.

IMPACT:

DNS caches are short lived and are generated by a recent DNS name-resolution event. By repeatedly monitoring DNS cache entries over a period of time, an attacker could gain a variety of information about the target network. For example, one could analyze Web-browsing habits of the users of a network. By querying for DNS MX record caches, one could check for email communication between two companies.
Information gathered from the DNS cache could lead to a variety of consequences ranging from an invasion of privacy to corporate espionage. The above mentioned paper presents a couple of attack scenarios where this vulnerability can be used.

SOLUTION:

Here is a suggested solution for the Microsoft Windows DNS server. One rigorous solution involves what is known popularly as a "split DNS" configuration.

The idea is to have two separate DNS servers, one for the DMZ/perimeter of the network that faces the public Internet, while the other is internal and

not publically accessible.
The external one has zone information about only the hosts in the DMZ region which need to be accessed from the Internet. It has no information about the internal hosts with non-routable addresses.
The internal one has all the authoritative information about the internal hosts, and also static entries for the services in the DMZ region (so internal users can access those if required).
Typically, the internal DNS server will be Active Directory integrated, with (secure) dynamic updates enabled.
The external DNS server will typically be a standalone (not integrated with the Active Directory) server without any dynamic DNS updates enabled.
To prevent the unrelated DNS cache-poisoning vulnerability, also configure the registry as explained in Microsoft Knowledge Base Article 241352 (http://support.microsoft.com/default.aspx?scid=kb;EN-US;241352) on both the DNS servers.
Both the DNS servers can be named with identical domain names, such as example.com without any conflicts.
The external DNS server should be set as a "forwarder" in the DNS settings of the internal DNS server. This means, for any DNS query (A/PTR) that the internal DNS server receives, that it is not able to resolve, it forwards it to the external DNS server for resolution.
Through the "DNS" MMC snap-in, Recursion should be enabled on the external DNS server, and disabled in the internal one. This prevents the internal DNS server from attempting to resolve DNS queries if the external one fails to do so.
To reinforce the last configuration, the internal DNS server should be set as a "slave" DNS server through the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" key's "IsSlave" value set to 1.
Finally, to prevent cache snooping on the external DNS server, create a "MaxCacheTtl" DWORD entry with value set to 1 under the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters" key of the external DNS server. This makes the TTL of any cached DNS entry on the external DNS server equal to 1 second, effectively disabling caching on it. Since for any query originating from the internal network, both the DNS servers cache the responses, performance is not affected at all even by disabling the external cache - repeated future DNS queries will be picked up by the internal DNS server and replied to from its cache.

This separates the external DNS proxy from the internal DNS cache, and prevents any DNS cache snooping from the public Internet.

For BIND and the understanding of the issue this URL will be helpful. http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf (http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server's cache timeout for IPv4 addresses is more than 3 sec.
Server's cache timeout for IPv6 addresses is more than 3 sec.

Information Gathered (78)

■■■□□ 3 Content-Security-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).
QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Content-Security-Policy HTTP Header missing on port 8014.
GET / HTTP/1.0
Host: dc2.enterate.com:8014

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 8014/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 8014.
GET / HTTP/1.0
Host: dc2.enterate.com:8014

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:53
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

■■□□□ 2 DNS Hierarchy of Target DNS Server Traced

QID:	45035
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/15/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This probe traces the hierarchy of the target DNS server. It first makes a non-recursive query to one of the root DNS servers (*.root-servers.net).

These servers point the scanner to the next level of DNS servers that handle the top-level domains, like ".com", and ".net". Then this lower-level DNS server is queried for the next-level DNS server and so on. This is repeated until a DNS server that is authoritative on the target hosts's FQDN domain (or has a cached DNS "A" record for the target) is found.
The hierarchy information is presented in the Result section below.
This information can be used to better map the chain of DNS servers from the root servers down to the actual target DNS server. This gives the flow of DNS information through the chain, and also it can help predict which DNS servers are authoritative on which domains.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Level 1: DNS server: B.ROOT-SERVERS.NET. (199.9.14.201)
Level 2: DNS server: b.gtld-servers.net. (192.33.14.30)
Level 3: DNS server: ns10.domaincontrol.com. (173.201.72.5)
Level 4: ns10.domaincontrol.com. knows nothing about dc2.enterate.com.

■■□□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0			593	
DCOM OXID Resolver	0.0			593	
DCOM Remote Activation	0.0			593	
DCOM System Activator	0.0			593	
Domain Name System	5.0	59188			

Microsoft Local Security Architecture	0.0	49669, 49667	49670	\pipe\8fde6c728f07f99c, \pipe\lsass
Microsoft LSA DS Access	0.0	49669, 49667	49670	
Microsoft Network Logon	1.0	49669, 49667	49670	\pipe\8fde6c728f07f99c, \pipe\lsass
Microsoft NT Directory DRS Interface	4.0	49669, 49667	49670	\pipe\8fde6c728f07f99c, \pipe\lsass
Microsoft Scheduler Control Service	1.0	49672		\PIPE\atsvc
Microsoft Security Account Manager	1.0	49669, 49667	49670	\pipe\lsass
Microsoft Service Control Service	2.0	59203		
Microsoft Task Scheduler	1.0	49672		\PIPE\atsvc
MS Wbem Transport IEnumWbemClassObject	0.0	49672		
MS Wbem Transport IWbemLevel1Login	0.0	49672		
MS Wbem Transport IWbemObjectSink	0.0	49672		
MS Wbem Transport IWbemServices	0.0	49672, 59194		
MS Windows DHCP Server (API 1)	1.0	59170		
MS Windows DHCP Server (API 2)	1.0	59170		
WinHttp Auto-Proxy Service	5.1			\PIPE\W32TIME_ALT
(Unknown Service)	1.0		593	
(Unknown Service)	1.0	49669, 49667	49670	
(Unknown Service)	0.0	49669, 49672, 59194, 49667, 59170	49670	
(Unknown Service)	0.0	49672		
(Unknown Service)	0.0		593	
(Unknown Service)	1.0	49672		
(Unknown Service)	2.0		593	
(Unknown Service)	0.0	49669, 49667	49670	
(Unknown Service)	1.0	49669, 49672, 49667	49670	\pipe\lsass
(Unknown Service)	0.0	49669, 49667	49670	\pipe\8fde6c728f07f99c, \pipe\lsass
(Unknown Service)	2.0	49669, 49667	49670	\pipe\8fde6c728f07f99c, \pipe\lsass
(Unknown Service)	1.0	49669, 49667	49670	\pipe\8fde6c728f07f99c, \pipe\lsass
(Unknown Service)	1.0	49664		
(Unknown Service)	1.0	49664		\PIPE\InitShutdown
(Unknown Service)	4.0	49672		
(Unknown Service)	2.0	49672		\PIPE\atsvc
(Unknown Service)	1.0	49672		\PIPE\atsvc
(Unknown Service)	1.0	49672		\pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	0.0	59194		
(Unknown Service)	1.0	59194		
(Unknown Service)	1.0			\pipe\LSM_API_service
(Unknown Service)	0.0			\pipe\LSM_API_service
Event log TCPIP	1.0	49665		\pipe\eventlog
DfsDs service	1.0			\PIPE\wkssvc
Remote Fw APIs	1.0	49674		

■■□□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 53, the host's uptime is 3 days, 22 hours, and 20 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

■■□□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.10.5	dc2.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 80, 111, 443, 1, 7.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-52,54-87,89-134,136-388,390-444,446-463,465-592,594-635,637-1705,1707-1999,
2001-2146,2148-2512,2514-2701,2703-2868,2870-3267,3270-3388,3390-3719,
3721-5630,5632-5984,5986-6128,6130-8013,8015-9388,9390-42423,42425-47000,
47002-49663,49666,49668,49671,49673,49675-59169,59171-59187,59189-59193,
59195-59202,59204-65535
```

1 LDAP Information Gathering

QID:	45016
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

RootDSE is a standard attribute defined in the LDAP Version 3.0 specification. RootDSE contains information about the directory server, including its capabilities and configuration. The search response will contain a standard set of information, which is defined in the following RFC:
RFC 2251-Lightweight Directory Access Protocol(v3) (http://www.cis.ohio-state.edu/htbin/rfc/rfc2251.html)
The root DSE (DSA-Specific Entry) data can be retrieved from an LDAPv3 server by performing a base-level search with a null BaseDN and filter ObjectClass=*. The root DSE publishes information about the LDAP server, including which LDAP versions it supports, any supported SASL mechanisms, supported controls, and the DN for its subschemaSubentry. In addition to server information, operational attributes may be exposed that allow for extended administration functionality.

IMPACT:

The information gathered can be used to launch further attacks against the system or network hosting the LDAP service.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
currentTime: 20210220053950.0Z
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=enterate,DC=co
 m
dsServiceName: CN=NTDS Settings,CN=DC2,CN=Servers,CN=broward_colo,CN=Sites,C
 N=Configuration,DC=enterate,DC=com
namingContexts: DC=enterate,DC=com
namingContexts: CN=Configuration,DC=enterate,DC=com
namingContexts: CN=Schema,CN=Configuration,DC=enterate,DC=com
namingContexts: DC=DomainDnsZones,DC=enterate,DC=com
namingContexts: DC=ForestDnsZones,DC=enterate,DC=com
defaultNamingContext: DC=enterate,DC=com
schemaNamingContext: CN=Schema,CN=Configuration,DC=enterate,DC=com
configurationNamingContext: CN=Configuration,DC=enterate,DC=com
rootDomainNamingContext: DC=enterate,DC=com
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.840.113556.1.4.801
supportedControl: 1.2.840.113556.1.4.473
supportedControl: 1.2.840.113556.1.4.528
supportedControl: 1.2.840.113556.1.4.417
supportedControl: 1.2.840.113556.1.4.619
supportedControl: 1.2.840.113556.1.4.841
supportedControl: 1.2.840.113556.1.4.529
supportedControl: 1.2.840.113556.1.4.805
supportedControl: 1.2.840.113556.1.4.521
supportedControl: 1.2.840.113556.1.4.970
supportedControl: 1.2.840.113556.1.4.1338
supportedControl: 1.2.840.113556.1.4.474
supportedControl: 1.2.840.113556.1.4.1339
supportedControl: 1.2.840.113556.1.4.1340
supportedControl: 1.2.840.113556.1.4.1413
supportedControl: 2.16.840.1.113730.3.4.9
```

```
supportedControl: 2.16.840.1.113730.3.4.10
supportedControl: 1.2.840.113556.1.4.1504
supportedControl: 1.2.840.113556.1.4.1852
supportedControl: 1.2.840.113556.1.4.802
supportedControl: 1.2.840.113556.1.4.1907
supportedControl: 1.2.840.113556.1.4.1948
supportedControl: 1.2.840.113556.1.4.1974
supportedControl: 1.2.840.113556.1.4.1341
supportedControl: 1.2.840.113556.1.4.2026
supportedControl: 1.2.840.113556.1.4.2064
supportedControl: 1.2.840.113556.1.4.2065
supportedControl: 1.2.840.113556.1.4.2066
supportedControl: 1.2.840.113556.1.4.2090
supportedControl: 1.2.840.113556.1.4.2205
supportedControl: 1.2.840.113556.1.4.2204
supportedControl: 1.2.840.113556.1.4.2206
supportedControl: 1.2.840.113556.1.4.2211
supportedControl: 1.2.840.113556.1.4.2239
supportedControl: 1.2.840.113556.1.4.2255
supportedControl: 1.2.840.113556.1.4.2256
supportedControl: 1.2.840.113556.1.4.2309
supportedLDAPVersion: 3
supportedLDAPVersion: 2
supportedLDAPPolicies: MaxPoolThreads
supportedLDAPPolicies: MaxPercentDirSyncRequests
supportedLDAPPolicies: MaxDatagramRecv
supportedLDAPPolicies: MaxReceiveBuffer
supportedLDAPPolicies: InitRecvTimeout
supportedLDAPPolicies: MaxConnections
supportedLDAPPolicies: MaxConnIdleTime
supportedLDAPPolicies: MaxPageSize
supportedLDAPPolicies: MaxBatchReturnMessages
supportedLDAPPolicies: MaxQueryDuration
supportedLDAPPolicies: MaxDirSyncDuration
supportedLDAPPolicies: MaxTempTableSize
supportedLDAPPolicies: MaxResultSetSize
supportedLDAPPolicies: MinResultSets
supportedLDAPPolicies: MaxResultSetsPerConn
supportedLDAPPolicies: MaxNotificationPerConn
supportedLDAPPolicies: MaxValRange
supportedLDAPPolicies: MaxValRangeTransitive
supportedLDAPPolicies: ThreadMemoryLimit
supportedLDAPPolicies: SystemMemoryLimitPercent
highestCommittedUSN: 7955423
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
dnsHostName: dc2.enterate.com
ldapServiceName: enterate.com:dc2$@ENTERATE.COM
serverName: CN=DC2,CN=Servers,CN=broward_colo,CN=Sites,CN=Configuration,DC=e
 nterate,DC=com
supportedCapabilities: 1.2.840.113556.1.4.800
supportedCapabilities: 1.2.840.113556.1.4.1670
supportedCapabilities: 1.2.840.113556.1.4.1791
supportedCapabilities: 1.2.840.113556.1.4.1935
supportedCapabilities: 1.2.840.113556.1.4.2080
supportedCapabilities: 1.2.840.113556.1.4.2237
isSynchronized: TRUE
isGlobalCatalogReady: TRUE
domainFunctionality: 7
forestFunctionality: 7
domainControllerFunctionality: 7
```

▮▯▯▯▯ 1 Active Directory / Windows Network Enumeration Through DNS Service Locator Records

QID:	45023
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/26/2004
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

The DNS server is participating in an Active Directory (Windows Network) domain. The server provides Service Locator Resource Records (SRV RR) to clients requesting them. These SRV RRs contain host names and port numbers for the Windows domain services like Domain Controllers, Global Catalog, Kerberos KDC, Kerberos "passwd" services. These services are required by a domain based on Active Directories, and are used by participating workstations during boot up and authentication.
This module gathers information from these SRV RRs about the Active Directory domain.

IMPACT:

Information gathered may be used to better map the network. Services listed are critical for the Active Directory based network to be available.

SOLUTION:

An effective firewall scheme can be used to shield the DNS server from non-participating or external hosts from querying the DNS server for these records.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
DC LDAP: Host = dc1.enterate.com, Port = 389 (TCP)
DC LDAP: Host = dc2.enterate.com, Port = 389 (TCP)
PDC LDAP: Host = dc1.enterate.com, Port = 389 (TCP)
Global Catalog LDAP: Host = dc2.enterate.com, Port = 3268 (TCP)
Global Catalog LDAP: Host = dc1.enterate.com, Port = 3268 (TCP)
DC Kerberos KDC: Host = dc1.enterate.com, Port = 88 (TCP)
DC Kerberos KDC: Host = dc2.enterate.com, Port = 88 (TCP)
LDAP: Host = dc1.enterate.com, Port = 389 (TCP)
LDAP: Host = dc2.enterate.com, Port = 389 (TCP)
Global Catalog: Host = dc1.enterate.com, Port = 3268 (TCP)
Global Catalog: Host = dc2.enterate.com, Port = 3268 (TCP)
Kerberos KDC: Host = dc2.enterate.com, Port = 88 (TCP)
Kerberos KDC: Host = dc1.enterate.com, Port = 88 (TCP)
Kerberos KDC: Host = dc2.enterate.com, Port = 88 (UDP)
Kerberos KDC: Host = dc1.enterate.com, Port = 88 (UDP)
Kpasswd: Host = dc2.enterate.com, Port = 464 (TCP)
Kpasswd: Host = dc1.enterate.com, Port = 464 (TCP)
Kpasswd: Host = dc2.enterate.com, Port = 464 (UDP)
Kpasswd: Host = dc1.enterate.com, Port = 464 (UDP)
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The

Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2374 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:16:13 GMT

▮▯▯▯▯ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
dc2.enterate.com	NTLM DNS

dc2.enterate.com	FQDN
DC2	NTLM NetBIOS

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:

Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.
```

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	53	0:01:57
TCP	135	0:07:26
TCP	389	0:00:08
TCP	445	0:00:10
TCP	593	0:00:45
TCP	636	0:01:00
TCP	3268	0:00:08
TCP	3269	0:01:00
TCP	3389	0:00:51
TCP	5985	0:29:09
TCP	8014	0:52:11
TCP	9389	0:01:55
TCP	47001	0:35:20
TCP	49664	0:05:13
TCP	49665	0:05:05
TCP	49667	0:05:05
TCP	49669	0:05:07
TCP	49670	0:00:45
TCP	49672	0:05:05
TCP	49674	0:05:05
TCP	59170	0:05:05
TCP	59188	0:05:05
TCP	59194	0:05:05
TCP	59203	0:05:05
UDP	53	0:00:13
UDP	123	0:01:24
UDP	464	0:00:07
UDP	61466	0:00:07

▮□□□□ 1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Microsoft Server Message Block (SMBv3) Compression Disabled

▮▯▯▯▯ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Enabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default
CIFS Version	SMB v1 NT LM 0.12

▮▯▯▯▯ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
53	domain	Domain Name Server	named udp
123	ntp	Network Time Protocol	ntp
464	kpasswd	kpasswd	Kerberos Password
61466	unknown	unknown	unknown

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
53	domain	Domain Name Server	DNS Server	
88	kerberos	Kerberos	Kerberos-5	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
389	ldap	Lightweight Directory Access Protocol	ldap	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
464	kpasswd	kpasswd	Kerberos Password	
593	http-rpc-epmap	HTTP RPC Ep Map	msrpc-over-http	
636	ldaps	ldap protocol over TLS/SSL (was sldap)	ldap over ssl	
3268	msft-gc	Microsoft Global Catalog	ldap	
3269	msft-gc-ssl	Microsoft Global Catalog with LDAP/SSL	ldap over ssl	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
8014	unknown	unknown	http over ssl	
9389	unknown	unknown	unknown	
47001	unknown	unknown	http	
49664	unknown	unknown	msrpc	
49665	unknown	unknown	msrpc	
49667	unknown	unknown	msrpc	
49669	unknown	unknown	msrpc	
49670	unknown	unknown	msrpc-over-http	
49672	unknown	unknown	msrpc	
49674	unknown	unknown	msrpc	
59170	unknown	unknown	msrpc	
59188	unknown	unknown	msrpc	
59194	unknown	unknown	msrpc	
59203	unknown	unknown	msrpc	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:36:40 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DC2

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045

Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1136324334 with a standard deviation of 604253956. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5198 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 53: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2
Duration: 25 milli seconds
```

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:40:08 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:40:13 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: dc2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:40:08 GMT
Connection: close
Content-Length: 315
```

▮□□□□ 1 SSL Server Information Retrieval port 636/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 636/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 636/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 636/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

▮▯▯▯▯ 1 SSL/TLS Protocol Properties port 636/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 636/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 636/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 636/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 Microsoft Windows Active Directory / Domain Controller Present port 636/tcp over SSL

QID:	45022
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Active Directory is present on the remote system. The system is running as a Domain Controller.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

1 SSL Certificate - Information port 636/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:

(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256

(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:

(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

■□□□□ 1 Microsoft Windows Active Directory / Domain Controller Present port 389/tcp

QID:	45022
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Active Directory is present on the remote system. The system is running as a Domain Controller.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:53:25 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:53:30 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: dc2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:53:25 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 3269/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮□□□□ 1 SSL Session Caching Information port 3269/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

▮□□□□ 1 SSL/TLS invalid protocol version tolerance port 3269/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

▮□□□□ 1 SSL/TLS Key Exchange Methods port 3269/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

■□□□□ 1 SSL/TLS Protocol Properties port 3269/tcp over SSL

QID: 38706
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended.

Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3269/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 3269/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3269/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3269/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1

(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13

(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:

(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

1 HTTP Methods Returned by OPTIONS Request port 8014/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
```

1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8014.

```
GET / HTTP/1.0
Host: dc2.enterate.com:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=99D5487683D33DF49B8FDB723B4C38DC; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Date: Sat, 20 Feb 2021 05:58:20 GMT
Connection: close
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 8014/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8014 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8014/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubDomains

1 List of Web Directories port 8014/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/css/	web page
/images/	web page
/images/default/	web page
/images/default/window/	web page

1 Default Web Page port 8014/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc2.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8014/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: dc2.enterate.com:8014



<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
</body>
</html>
```

1 SSL Server Information Retrieval port 8014/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8014/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8014/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8014/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low

■□□□□ 1 SSL/TLS Protocol Properties port 8014/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 8014/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8014/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 8014/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT

(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:

(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8014/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which

is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.10.5:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.17.10.5:8014



HTTP/1.1 200
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AGENTJSESSIONID=1F745DF869630E40B484C1E436A5E334; Path=/; Secure; HttpOnly
Accept-Ranges: bytes
ETag: W/"1750-1528734626000"
Last-Modified: Mon, 11 Jun 2018 16:30:26 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Date: Sat, 20 Feb 2021 06:14:13 GMT

6d3
<!doctype html>
<html>
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta http-equiv="x-ua-compatible" content="IE=EDGE">
    <meta name="gwt:property" content="locale=en">
    <link rel="Shortcut Icon" href="images/5.0/websiteicon.ico">
    <link rel="stylesheet" type="text/css" href="css/gxt-all.css" />
    <link type="text/css" rel="stylesheet" href="asedl/css/as-edl.css">
    <link type="text/css" rel="stylesheet" href="css/common.css">
    <link type="text/css" rel="stylesheet" href="index.css">

    <title></title>
    <script type="text/javascript" language="javascript" src="contents/contents.nocache.js?version=D2DVersion"></script>
</head>
<body>
    <div style="display: none;">
        <img src="images/default/window/icon-error.gif"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/top-bottom.png"></img>
        <img src="images/default/window/left-corners.png"></img>
        <img src="images/default/window/right-corners.png"></img>
        <img src="images/default/window/left-right.png"></img>
    </div>
    <noscript><table border="0" width="90%" height="100%" align="center" cellspacing="30"><tbody><tr><td align="center" valign="top"><div
class="noscript_class">__noscript_html_text__</div></td></tr></tbody></table></noscript>
 <iframe src="javascript:''" id="__gwt_historyFrame" tabIndex='-1' style="position:absolute;width:0;height:0;border:0;top=50"></iframe>
    <div id="Div_Contents"></div>
    <script src="js/arcserve.js"></script>
```

```
</body>
</html>

0

HTTP/1.1 404
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Length: 0
Date: Sat, 20 Feb 2021 06:14:13 GMT
```

■□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH

ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low

ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

▮□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:

(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:

(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.10.20 (util17-2.enterate.com, UTIL17-2) Windows 2016

Potential Vulnerabilities (1)

■■■□□ 3 Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake) port 9300/tcp over SSL

QID:	13607
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/02/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Transport Layer Security (TLS) master secret is not cryptographically bound to important session parameters such as the server certificate. Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same.
Note: this attacks are reminiscent of the renegotiation attacks of 2009 [Ray, Rex] (CVE-2009-3555).
QID Detection Logic(Un-Authenticated):
This QID checks for web response coming from vulnerable host.
Note:Please refer Detection POC (https://github.com/Tripwire-VERT/TLS_Extended_Master_Checker) for more details of the detection logic

IMPACT:

On successful exploitation it becomes vulnerable to a man-in-the-middle attack, where the attacker can simply forward messages back and forth between the client and server.

SOLUTION:

Refer to the Workarounds available.
Workaround:To re-mediate this vulnerability these bug workaround (https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_options.html) options are available.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Host:172.17.10.20:9300 is vulnerable to TLS triple handshake

Information Gathered (103)

■■■□□ 3 DEFLATE Data Compression Algorithm Used for HTTPS

QID:	42416
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/09/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.
DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.
This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 06:14:36 GMT
Content-Length: 609

_1F_8B_08_00_00_00_00_00_04_00_ED_BD_07`_1CI_96%&/m_CA{_7FJ_F5J_D7_E0t_A1_08_80`_13
$_D8_90@_10_EC_C1_88_CD_E6_92_EC_1DiG#)_AB*_81_CAeVe]f_16@_CC_ED_9D_BC_F7_DE{_EF_BD_F7_DE{_EF_BD_F7_BA;
_9DN'_F7_DF_FF?\fd_01l_F6_CEJ_DA_C9_9E!_80_AA_C8_1F?~|_1F?"_1E_FF_AEO_BF<y_F3_FB_BC<M_E7_ED_A2L_~
_F5_E4_F9_D9I_FA_D1_F6_DD_BB_DF_BDwr_F7_EE_D37O_D3_DF_FB_DBo_BEx_9E_EE_8Ew_D2_D7m]L_DB_BBwO_|
_94~4o_DB_D5_A3_BBw_AF_AE_AE_C6W_F7_C6U}q_F7_CD_AB_BB_EF_00e_17_AF_E9_AF_DB_BF3_9E_B5_B3_8F_8E~_E3_E41>L_DF-
_CAe_F3Y_04_C2_EE_C3_87_0F_E5Ei_9Cg3_FC\_E4mF_F8_B5_AB_ED_FC_17_AD_8B_CB_CF>:_A9_96m_BEl_B7_DF\
_AF_F2_8F_D2_A9_FC_F5_D9Gm_FE_AE_BD_8B_B7_0F_D3_E9<_AB_9B_BC_FD_ACh_AA_ED_83_83_FB_0F_B7w?J_EF_02V[_B4e~tv_F6:
_FDn_B1_9CUWM_FA:_AF/_F3_FA_F1]_F9_86_9A4_EDu_99_A7-_C1V_90_D3_A6a|~
_D7_ED_ED_DF8_99T_B3_EB_F4_17_FF_C6_C9_8FM_AB_B2_AA_1F_FD_F8_0E?_87_F4_C1$_9B_BE_BD_A8_AB_F5r_B6m_BF{_B0w_F2)
_BE[d_F5E_B1|_84v_BF_E47N~_E3_E4_C7_81tV,_F3_9Aa_C9_D7_DBe~_DE>_CA_D6mE_CD_CCguq1w_1F_02_9F_ED_AC,.
_96_8F_A64_E6_BC_C6_87_0C1K_8B_C5_05_03_9BT_F5,_AF_1F-_ABeN_DF_F2_97_DB_DB_C0_FF._8F_8C_7F3_A4_C5h_F0sV\
_A6_C5_EC_B3_8F,Z<`_A2z_9D_9F_DB_99_BA_A8_C6_8BbZWMu_DE_8E_A7_D5_E2_EE_F9UY,_DF_DE_FD=_F0/
_BD_FD_E9_A7_BB_F7_0E~a_B6X_1DN_CB)_FD_BD_F3n_7F_E7_E1GG_8F_81XSO?_FB_A8(_9A_A6_CD_EAv_BCZ^|_94f%
_CD_19_CD_C4G_E9U1k_E7_9F}_F4_F0_D3_9D_8F_D2y_8E_01_7F_F6_D1_A7;
_F4_C7_DD_A3_C7w3`r_97_10_E4_9F_06a_9E_E7_A3_FF_07_AA_C0:_88_BF_02

HTTP/1.1 200 OK
Content-Type: text/html
Content-Encoding: gzip
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
```

```
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 06:14:43 GMT
Content-Length: 609
```

```
_1F_8B_08_00_00_00_00_00_04_00_ED_BD_07`_1CI_96%&/m_CA{_7FJ_F5J_D7_E0t_A1_08_80`_13
$_D8_90@_10_EC_C1_88_CD_E6_92_EC_1DiG#)_AB*_81_CAeVe]f_16@_CC_ED_9D_BC_F7_DE{_EF_BD_F7_DE{_EF_BD_F7_BA;
_9DN'_F7_DF_FF?\fd_01l_F6_CEJ_DA_C9_9E!_80_AA_C8_1F?~|_1F?"_1E_FF_AEO_BF<y_F3_FB_BC<M_E7_ED_A2L_~
_F5_E4_F9_D9l_FA_D1_F6_DD_BB_DF_BDwr_F7_EE_D37O_D3_DF_FB_DBo_BEx_9E_EE_8Ew_D2_D7m]L_DB_BBwO_|
_94~4o_DB_D5_A3_BBw_AF_AE_AE_C6W_F7_C6U}q_F7_CD_AB_BB_EF_00e_17_AF_E9_AF_DB_BF3_9E_B5_B3_8F_8E~_E3_E41>L_DF-
_CAe_F3Y_04_C2_EE_C3_87_0F_E5Ei_9Cg3_FC\_E4mF_F8_B5_AB_ED_FC_17_AD_8B_CB_CF>:_A9_96m_BEl_B7_DF\
_AF_F2_8F_D2_A9_FC_F5_D9Gm_FE_AE_BD_8B_B7_0F_D3_E9<_AB_9B_BC_FD_ACh_AA_ED_83_83_FB_0F_B7w?J_EF_02V[_B4e~tv_F6:
_FDn_B1_9CUWM_FA:_AF/_F3_FA_F1]_F9_86_9A4_EDu_99_A7-_C1V_90_D3_A6a|~
_D7_ED_ED_DF8_99T_B3_EB_F4_17_FF_C6_C9_8FM_AB_B2_AA_1F_FD_F8_0E?_87_F4_C1$_9B_BE_BD_A8_AB_F5r_B6m_BF{_B0w_F2)
_BE[d_F5E_B1|_84v_BF_E47N~_E3_E4_C7_81tV,_F3_9Aa_C9_D7_DBe~_DE>_CA_D6mE_CD_CCguq1w_1F_02_9F_ED_AC,.
_96_8F_A64_E6_BC_C6_87_0C1K_8B_C5_05_03_9BT_F5,_AF_1F-_ABeN_DF_F2_97_DB_DB_C0_FF._8F_8C_7F3_A4_C5h_F0sV\
_A6_C5_EC_B3_8F,Z<`_A2z_9D_9F_DB_99_BA_A8_C6_8BbZWMu_DE_8E_A7_D5_E2_EE_F9UY,_DF_DE_FD=_F0/
_BD_FD_E9_A7_BB_F7_0E~a_B6X_1DN_CB)_FD_BD_F3n_7F_E7_E1GG_8F_81XSO?_FB_A8(_9A_A6_CD_EAv_BCZ^|_94f%
_CD_19_CD_C4G_E9U1k_E7_9F}_F4_F0_D3_9D_8F_D2y_8E_01_7F_F6_D1_A7;
_F4_C7_DD_A3_C7w3`r_97_10_E4_9F_06a_9E_E7_A3_FF_07_AA_C0:_88_BF_02
```

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: util17-2.enterate.com
```

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:80
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCOM System Activator	0.0	49702			
Microsoft Local Security Architecture	0.0	49675, 49667			
Microsoft LSA DS Access	0.0	49675, 49667			
Microsoft Network Logon	1.0	49675, 49667			
Microsoft Scheduler Control Service	1.0	49702			
Microsoft Security Account Manager	1.0	49675, 49667			
Microsoft Task Scheduler	1.0	49702			
MS Wbem Transport IEnumWbemClassObject	0.0	49702			
MS Wbem Transport IWbemLevel1Login	0.0	49702			
MS Wbem Transport IWbemObjectSink	0.0	49702			
MS Wbem Transport IWbemServices	0.0	49702			
(Unknown Service)	1.0	49675, 49667			
(Unknown Service)	0.0	49702			
(Unknown Service)	1.0	49702			
(Unknown Service)	0.0	49675, 49667			
(Unknown Service)	2.0	49675, 49667			
(Unknown Service)	1.0	49664			
(Unknown Service)	4.0	49702			
(Unknown Service)	2.0	49702			

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in

various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 80, the host's uptime is 4 days, 12 hours, and 7 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

2 Microsoft ASP.NET HTTP Handlers Enumerated port 80/tcp

QID:	12033
Category:	CGI

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 80/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

2 Microsoft ASP.NET HTTP Handlers Enumerated port 443/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.

The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,

■■□□□ 2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 443/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:
Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:
Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

2 Microsoft ASP.NET HTTP Handlers Enumerated port 8531/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,.Soap,

2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 8531/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Web Server HTTP Protocol Versions port 8531/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8531 port.GET / HTTP/1.1

2 Microsoft ASP.NET HTTP Handlers Enumerated port 8530/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 8530/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").

Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,.Soap,

■■□□ 2 Web Server HTTP Protocol Versions port 8530/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 8530 port.GET / HTTP/1.1

■■□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.10.20	util17-2.enterate.com

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 1, 7, 11.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-134,136-442,444,446-512,515-1705,1707-1999,2001-2146,2148-2512,
2514-2701,2703-2868,2870-3388,3390-5630,5632-5984,5986-6128,6130-8529,
8532-9299,9301-11744,11746-42423,42425-47000,47002-49663,49666,49668-49674,
49676-49700,49703-49705,49707-49731,49733-65535

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2404 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:17:11 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
util17-2.enterate.com	NTLM DNS
util17-2.enterate.com	FQDN
UTIL17-2	NTLM NetBIOS

▮□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

■□□□□ 1 Scan Activity per Port

QID:	45426

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:39:56
TCP	135	0:07:27
TCP	443	0:48:40
TCP	445	0:00:01
TCP	513	0:04:18
TCP	514	0:13:33
TCP	3389	0:00:51
TCP	5985	0:28:51
TCP	8530	0:35:34
TCP	8531	0:49:51
TCP	9300	0:01:00
TCP	47001	0:29:26
TCP	49664	0:05:05
TCP	49665	0:05:06
TCP	49667	0:05:11
TCP	49675	0:05:16
TCP	49701	0:05:05
TCP	49702	0:05:11
TCP	49706	0:12:37
TCP	49732	0:05:05

1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Microsoft Server Message Block (SMBv3) Compression Disabled
```

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
513	login	remote login a la telnet	unknown	
514	shell	cmd	unknown	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
8530	unknown	unknown	http	
8531	unknown	unknown	http over ssl	
9300	unknown	unknown	unknown over ssl	
47001	unknown	unknown	http	
49664	unknown	unknown	msrpc	
49665	unknown	unknown	msrpc	
49667	unknown	unknown	msrpc	
49675	unknown	unknown	msrpc	
49701	unknown	unknown	msrpc	
49702	unknown	unknown	msrpc	
49706	unknown	unknown	unknown	
49732	unknown	unknown	msrpc	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:11 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

UTIL17-2

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1261598197 with a standard deviation of 469544250. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5090 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 80: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 23 milli seconds
```

■□□□□ 1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com


HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Server: Microsoft-IIS/10.0
```

```
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:39:52 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 80/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:40:56 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 HTTP Methods Returned by OPTIONS Request port 80/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Allow: OPTIONS, TRACE, GET, HEAD, POST

■□□□□ 1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

```
GET / HTTP/1.0
Host: util17-2.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:39:52 GMT
Connection: keep-alive
Content-Length: 703
```

▮▯▯▯▯ 1 Referrer-Policy HTTP Security Header Not Detected port 80/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 80 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 80/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

1 Microsoft IIS ASP.NET Version Obtained port 80/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
X-AspNet-Version: 4.0.30319

1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/aspnet_client/	brute force
/rpc/	brute force

1 Web Server Unconfigured - Default Install Page Present port 80/tcp

QID:	87089
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/28/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The web server uses its default welcome page.
This may mean that the web server is not used or is not properly configured.
QID Detection Logic (unauthenticated):
The Detection reviews the default page.

IMPACT:

N/A

SOLUTION:
Configure the web server to not display the default welcome page or disable the HTTP service if you do not use it.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:39:52 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:43:58 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
```

```
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:45:48 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
```

```
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

▮□□□□ 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					

SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS

TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 443/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

■□□□□ 1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT

(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)

(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/

commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 443/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 443.

```
GET / HTTP/1.0
Host: util17-2.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:43:58 GMT
Connection: keep-alive
Content-Length: 703
```

1 Referrer-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add

secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 443 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubdomains

■□□□□ 1 Microsoft IIS ASP.NET Version Obtained port 443/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
X-AspNet-Version: 4.0.30319

1 List of Web Directories Requiring Authentication port 443/tcp

QID:	86671
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The service has identified a list of Web directories which require authentication to access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directories Requiring Authentication
/rpc/

1 List of Web Directories port 443/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/aspnet_client/	brute force
/rpc/	brute force

■□□□□ 1 Web Server Unconfigured - Default Install Page Present port 443/tcp

QID:	87089
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/28/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The web server uses its default welcome page.
This may mean that the web server is not used or is not properly configured.
QID Detection Logic (unauthenticated):
The Detection reviews the default page.

IMPACT:
N/A

SOLUTION:
Configure the web server to not display the default welcome page or disable the HTTP service if you do not use it.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 17 Jul 2018 18:40:19 GMT
```

```
Accept-Ranges: bytes
ETag: "667c9d9cfd1dd41:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:43:58 GMT
Connection: keep-alive
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 8531/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

1 HTTP Response Method and Header Information Collected port 8531/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 8531.

GET / HTTP/1.0
Host: util17-2.enterate.com:8531


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:49:55 GMT
Connection: keep-alive
Content-Length: 1233
```

1 HTTP Strict Transport Security (HSTS) Support Detected port 8531/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

1 Microsoft IIS ASP.NET Version Obtained port 8531/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

X-AspNet-Version: 4.0.30319

■□□□□ 1 List of Web Directories port 8531/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/content/	brute force
/Content/	brute force

■□□□□ 1 Default Web Page port 8530/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com:8530



HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:54:00 GMT
Connection: keep-alive
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8530/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com:8530



HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:55:31 GMT
Connection: keep-alive
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 8530/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

1 HTTP Response Method and Header Information Collected port 8530/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8530.

```
GET / HTTP/1.0
Host: util17-2.enterate.com:8530



HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:54:00 GMT
Connection: keep-alive
Content-Length: 1233
```

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 8530/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000; includeSubdomains

■□□□□ 1 Microsoft IIS ASP.NET Version Obtained port 8530/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
X-AspNet-Version: 4.0.30319
```

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8530/tcp

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.10.20:8530

GET /Q_Evasive/ HTTP/1.1
Host:172.17.10.20:8530



HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 06:14:05 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
HTTP/1.1 404 Not Found
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 06:14:05 GMT
Content-Length: 1245

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>404 - File or directory not found.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>404 - File or directory not found.</h2>
  <h3>The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

1 List of Web Directories port 8530/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/content/	brute force
/Content/	brute force

1 Default Web Page port 8531/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com:8531



HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:49:55 GMT
Connection: keep-alive
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8531/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com:8531



HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 05:51:18 GMT
Connection: keep-alive
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
```

```
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

1 SSL Server Information Retrieval port 8531/tcp over SSL

QID: 38116
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH

AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8531/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 8531/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the

target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8531/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low

ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 8531/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 8531/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

▮□□□□ 1 SSL Certificate Transparency Information port 8531/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8531/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8531/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:

(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)

(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:

(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8531/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.10.20:8531

GET /Q_Evasive/ HTTP/1.1
Host:172.17.10.20:8531



HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 06:14:05 GMT
Content-Length: 1233

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>403 - Forbidden: Access is denied.</h2>
  <h3>You do not have permission to view this directory or page using the credentials that you supplied.</h3>
 </fieldset></div>
</div>
</body>
</html>
HTTP/1.1 404 Not Found
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
Date: Sat, 20 Feb 2021 06:14:05 GMT
Content-Length: 1245

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>404 - File or directory not found.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>404 - File or directory not found.</h2>
  <h3>The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:57:25 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com:5985
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:57:49 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: util17-2.enterate.com:5985


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:57:25 GMT
Connection: close
Content-Length: 315
```

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:01:05 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:02:00 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: util17-2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:01:05 GMT
Connection: close
Content-Length: 315
```

▮▯▯▯▯ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					

SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮□□□□ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS

TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT

(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)

(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/

commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad

(1) a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.10.21 (util17-3.enterate.com, UTIL17-3) Windows 2016

Information Gathered (101)

■■■□□ 3 DEFLATE Data Compression Algorithm Used for HTTPS

QID:	42416
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/09/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.
DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.
This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 302 Found
Date: Sat, 20 Feb 2021 06:14:51 GMT
Server: Symantec Endpoint Protection Manager
Content-Encoding: gzip
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' 172.17.10.21:8443
X-Frame-Options: ALLOW-FROM https://172.17.10.21:8443
X-Content-Type-Options: nosniff
location: https://util17-3:8445/Reporting/login/NoJavascript.php
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

16
_1F_8B_08_00_00_00_00_00_00_0B_E3_E5_02_00_AC_85_A2_14_02_00_00_00
0


HTTP/1.1 302 Found
```

```
Date: Sat, 20 Feb 2021 06:14:51 GMT
Server: Symantec Endpoint Protection Manager
Content-Encoding: deflate
Vary: Accept-Encoding
Content-Security-Policy: frame-ancestors 'self' 172.17.10.21:8443
X-Frame-Options: ALLOW-FROM https://172.17.10.21:8443
X-Content-Type-Options: nosniff
location: https://util17-3:8445/Reporting/login/NoJavascript.php
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

a
x_9C_E3_E5_02_00_00&_00_18
0
```

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 8443/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 8443.
GET / HTTP/1.0
Host: util17-3.enterate.com:8443
```

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U6483:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:

Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCOM System Activator	0.0	49700			
Microsoft Local Security Architecture	0.0	49666, 49667			
Microsoft LSA DS Access	0.0	49666, 49667			
Microsoft Network Logon	1.0	49666, 49667			
Microsoft Scheduler Control Service	1.0	49700			
Microsoft Security Account Manager	1.0	49666, 49667			
Microsoft Task Scheduler	1.0	49700			
MS Wbem Transport IEnumWbemClassObject	0.0	49700			
MS Wbem Transport IWbemLevel1Login	0.0	49700			
MS Wbem Transport IWbemObjectSink	0.0	49700			
MS Wbem Transport IWbemServices	0.0	49700			
(Unknown Service)	1.0	49666, 49667			
(Unknown Service)	0.0	49700			
(Unknown Service)	1.0	49700			
(Unknown Service)	0.0	49666, 49667			
(Unknown Service)	2.0	49666, 49667			
(Unknown Service)	1.0	49664			
(Unknown Service)	4.0	49700			
(Unknown Service)	2.0	49700			

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 443, the host's uptime is 4 days, 3 hours, and 59 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe.
Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1
```

■■□□□ 2 Web Server HTTP Protocol Versions port 8443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 8443 port.GET / HTTP/1.1
```

2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1
```

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8014/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8014 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 8446/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8446 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 8445/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8445 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.10.21	util17-3.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 1, 7.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2512,2514-2701,2703-2868,
2870-3388,3390-5630,5632-5984,5986-6128,6130-8013,8015-8442,8444,8447-33121,
33123-42423,42425-47000,47002-49663,49668-49698,49701-49702,49704-49705,
49707-49708,49710-65535
```

■□□□□ 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2733 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:22:40 GMT

■□□□□ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
util17-3.enterate.com	NTLM DNS
util17-3.enterate.com	FQDN
UTIL17-3	NTLM NetBIOS

1 Java Remote Method Invocation Detected

QID:	45186
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/23/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Java Remote Method Invocation or Java RMI, is a mechanism that allows one to invoke a method on an object that exists in another address space.
Java RMI is running on target host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Service name: Java RMI is running  on TCP port 49709.
Service name: Java RMI is running  on TCP port 49706.
```

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering

CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:

Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

■□□□□ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:07:50
TCP	443	0:42:43
TCP	445	0:00:02
TCP	3389	0:00:52

TCP	5985	0:31:58
TCP	8014	0:34:16
TCP	8443	0:41:12
TCP	8445	0:47:39
TCP	8446	0:49:58
TCP	47001	0:33:06
TCP	49664	0:05:05
TCP	49665	0:05:22
TCP	49666	0:05:05
TCP	49667	0:05:16
TCP	49699	0:05:05
TCP	49700	0:05:08
TCP	49703	0:05:05
TCP	49706	0:04:42
TCP	49709	0:04:28

■□□□□ 1 Java RMI Distributed Garbage-Collection Service Detected

QID:	48074
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Java RMI services can be exposed over network using TCP sockets. Every RMI service is identified by an object number.
Garbage-Collection Service (2 - DGC_ID) is detected on remote RMI service.
QID Detection Logic(Unauthenticated):
This QID sends a Java DGC RMI payload to the remote service.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Java RMI Distributed Garbage-Collection Service Detected on port 49709
Java RMI Distributed Garbage-Collection Service Detected on port 49706
```

■□□□□ 1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Microsoft Server Message Block (SMBv3) Compression Disabled

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
8014	unknown	unknown	http	
8443	unknown	unknown	http over ssl	
8445	unknown	unknown	http over ssl	
8446	unknown	unknown	http over ssl	
47001	unknown	unknown	http	
49664	unknown	unknown	msrpc	
49665	unknown	unknown	msrpc	
49666	unknown	unknown	msrpc	
49667	unknown	unknown	msrpc	
49699	unknown	unknown	msrpc	
49700	unknown	unknown	msrpc	
49703	unknown	unknown	msrpc	
49706	unknown	unknown	RMIRegistry	
49709	unknown	unknown	RMIRegistry	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:09 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

UTIL17-3

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1191426164 with a standard deviation of 495389306. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5112 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 22 milli seconds
```

■□□□□ 1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com



HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 05:39:37 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 198
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
```

```
<h1>Not Found</h1>
<p>The requested URL / was not found on this server.</p>
</body></html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com



HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 05:40:18 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 198
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL / was not found on this server.</p>
</body></html>
```

■□□□□ 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-CAMELLIA128-SHA	DH	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
DHE-RSA-CAMELLIA256-SHA	DH	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH

AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the

target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp384r1	384	yes	192	low

ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	brainpoolp512r1	512	yes	256	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	brainpoolp384r1	384	yes	192	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low
ECDHE	brainpoolp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes

Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/

(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36

(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

1 Web Server Supports HTTP Request Pipelining port 443/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.10.21:443

GET /Q_Evasive/ HTTP/1.1
Host:172.17.10.21:443



HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 06:13:34 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 198
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL / was not found on this server.</p>
</body></html>
HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 06:13:34 GMT
```

```
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 208
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /Q_Evasive/ was not found on this server.</p>
</body></html>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 443.

```
GET / HTTP/1.0
Host: util17-3.enterate.com


HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 05:39:37 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 198
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

1 HTTP Response Method and Header Information Collected port 8443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8443.

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8443



HTTP/1.1 200 OK
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: frame-ancestors 'self'
Strict-Transport-Security: max-age=31536000;includeSubDomains
X-Frame-Options: DENY
Set-Cookie: JSESSIONID=304E64148D385558B24CA592610A5151; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
Date: Sat, 20 Feb 2021 05:44:20 GMT
Connection: close
Server: SEPM
```

1 Referrer-Policy HTTP Security Header Not Detected port 8443/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 8443 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 8443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Strict-Transport-Security: max-age=31536000;includeSubDomains

1 List of Web Directories port 8443/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/console/	brute force

1 Default Web Page port 8443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8443




<!--
SYMANTEC:     Copyright (c) 2019 Symantec Corporation. All rights reserved.

THIS SOFTWARE CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF SYMANTEC CORPORATION.  USE,
DISCLOSURE OR REPRODUCTION IS PROHIBITED WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF SYMANTEC
CORPORATION.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in
FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer
Software - Restricted Rights" and DFARS 227.7202, Rights in "Commercial Computer Software or Commercial
Computer Software Documentation," as applicable, and any successor regulations, whether delivered by
Symantec as on premises or hosted services.  Any use, modification, reproduction release, performance,
display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely
in accordance with the terms of this Agreement.
-->









<html>
    <head>
        <META HTTP-EQUIV="content-type" CONTENT="text/html; charset=UTF-8">
  <!-- VBScript support is removed from IE. Refer following links
    http://msdn.microsoft.com/en-us/library/windows/apps/Hh700404.aspx indicates that support was removed from the ExecScript API. http://msdn.
microsoft.com/en-us/library/ie/dn384057(v=vs.85).aspx explains that it's removed from IE11 Edge mode in the Internet Zone.
    So if we want to run VBScript on IE, we need to add the following to the HEAD tag, this will ensure VBScript ca run on IE.
    e.g. META tag to be added to HEAD tag.
    <META http-equiv="x-ua-compatible" content="IE=10">
  -->
  <META http-equiv="X-UA-Compatible" content="IE=8" >
        <title>Symantec Endpoint Protection Manager</title>

  <SCRIPT LANGUAGE="JavaScript">
   if (top.frames.length > 0) {
    top.location=self.document.location;
   }
  </SCRIPT>

  <!-- First, determine if user agent is IE or Netscape browser -->
  <SCRIPT LANGUAGE="JavaScript">
   var browserName2 = "Unsupported";
   var browserName = getBrowserName();
   function getBrowserName() {
    var browserNameValue = 'Other';
    var userAgent = navigator.userAgent.toLowerCase();
    if (userAgent.indexOf('edge') >= 0) {
     browserNameValue = 'Edge';
     browserName2 = "Microsoft Edge";
    } else if (userAgent.indexOf('trident') >= 0) {
     browserNameValue = 'MSIE';
     browserName2 =  "Microsoft Internet Explorer";
    } else if (userAgent.indexOf('firefox') >= 0) {
     browserNameValue = 'Firefox';
     browserName2 = "Mozilla Firefox";
    } else if (userAgent.indexOf('chrome') >= 0 && userAgent.indexOf('safari') >= 0 && userAgent.indexOf('webkit') >= 0 && userAgent.indexOf('edge')
== -1 && userAgent.indexOf('opera') == -1 && userAgent.indexOf('opr') == -1) {
     browserNameValue = 'Chrome'
     browserName2 = "Google Chrome";
    } else if (userAgent.indexOf('opera') >= 0 || (userAgent.indexOf('chrome') >= 0 && userAgent.indexOf('safari') >= 0 && userAgent.indexOf('opr') >=
0)) {
     browserNameValue = 'Opera'
     browserName2 = "Opera";
    }
    return browserNameValue;
   }

   var osIs64Bit = is64BitOS();
   function is64BitOS() {
    var userAgent = navigator.userAgent.toLowerCase();
    var is64Bit = (userAgent.indexOf('win64; x64') >= 0 || userAgent.indexOf('wow64') >= 0);
    return is64Bit;
   }

   var browserIs64Bit = is64BitBrowser();
   function is64BitBrowser() {
    var userAgent = navigator.userAgent.toLowerCase();
    var is64Bit = (userAgent.indexOf('win64; x64') >= 0);
    return is64Bit;
   }

   var javaPluginInstalled = isJavaPluginDetected();
   function isJavaPluginDetected() {
    var javaPluginDetected = false;
    if (navigator.mimeTypes) {
     // Why are we not checking navigator.mimeTypes.length here?
     // Answer: Recent 64-bit Firefox browser returns '0' for navigator.mimeTypes.length where as returns
     // 'specific value for navigator.mimeTypes['application/x-java-jnlp-file']. So checking navigator.mimeTypes.length > 0
     // is blocking us from detecting java mime type.
     if (navigator.mimeTypes['application/x-java-jnlp-file'] || navigator.mimeTypes['application/x-java-vm']) {
      javaPluginDetected = true;
     }
    }
    return javaPluginDetected;
   }
  </SCRIPT>

  <SCRIPT LANGUAGE="JavaScript">
         var javaws15Installed=0;
         var javaws16Installed=0;
   var javaws17Installed=0;
   var javaws18Installed=0;
   var isIE = "false";
   if (browserName == "MSIE") {
    isIE = "true";
   }

   if (javaPluginInstalled) {
    javaws15Installed=1;
    javaws16Installed=1;
    javaws17Installed=1;
    javaws18Installed=1;
         }
      </SCRIPT>

      <!-- Now, if it is IE on Windows platform, we check to see which version of JWS is installed -->
      <!-- What happens with the VBScript in non-IE browser? Answer: This block won't get executed -->
      <SCRIPT LANGUAGE="VBScript">
         on error resume next
         If isIE = "true" Then
                 If Not(IsObject(CreateObject("JavaWebStart.isInstalled.1.5.0.0"))) Then
                         javaws15Installed = 0
                 Else
                         javaws15Installed = 1
                 End If
                 If Not(IsObject(CreateObject("JavaWebStart.isInstalled.1.6.0.0"))) Then
```

```
                              javaws16Installed = 0
                    Else
                              javaws16Installed = 1
                    End If
     If Not(IsObject(CreateObject("JavaWebStart.isInstalled.1.7.0.0"))) Then
                              javaws17Installed = 0
                    Else
                              javaws17Installed = 1
     End If
     If Not(IsObject(CreateObject("JavaWebStart.isInstalled.1.8.0.0"))) Then
                              javaws18Installed = 0
                    Else
                              javaws18Installed = 1
     End If
            End If
        </SCRIPT>
    </head>

    <body style="font-family: Arial, Helvetica, sans-serif;
                 font-size: 12px;">

        <SCRIPT LANGUAGE="JavaScript">
            if ( javaws18Installed ) {
                document.write('<applet code="com.sygate.scm.server.servlet.JavaVersionCheck" width="1" height="1" archive="scm-version-check.jar"
name="JavaVersionCheck"><param name="permissions" value="all-permissions"/><param name="minimumVersion" value="1.8.0_221"></applet>
');
                try {
                    var sysJava = JavaVersionCheck.isValidVersion();
                    if ( sysJava ) {
                        javaws18Installed = 1;
                    } else {
                        javaws18Installed = 0;
                    }
                } catch( e ) {
                    //alert("DEBUG: Applet execution throws following error: " + e.description);
                    // Applet can be executed if the remote computer has required JRE version installed. If installed JRE
     // is less than the required JRE version we may experience runtime issues such as API not found etc.
                    javaws18Installed = 0;
                }
            }
        </SCRIPT>

  <NOSCRIPT>
      <div style="background-color:#FFCC00;font-size:20pt;text-align:center">
          You must have JavaScript enabled to use this Web page.
      </div>
  </NOSCRIPT>

  <div id="supportedBrowsersMsg" style="background-color:#FDBB30;font-size:16pt;text-align:center;visibility:hidden">
         You are using an older browser version and might experience issues using this browser version to log on to the Web Console. See the
supported browser list under Web Console.
     </div>

  <!-- Web console is only supported on IE7 and later -->
        <SCRIPT LANGUAGE="JavaScript">
     if (isIE == "true") {
   var ix;
      var nAgt = navigator.userAgent;
   var verOffset=nAgt.indexOf("Trident");
   var fullVersion = nAgt.substring(verOffset+8);
   var baseversion;
   if ((ix=fullVersion.indexOf(";"))!=-1) fullVersion=fullVersion.substring(0,ix);

   //get the integer part
   if ((ix=fullVersion.indexOf("."))!=-1) baseversion=fullVersion.substring(0,ix);
   if (parseInt(baseversion) < 7) {
    document.getElementById("supportedBrowsersMsg").style.visibility = "visible";
   }
     }
        </SCRIPT>


        <SCRIPT LANGUAGE="JavaScript">

   // Client-side check if cookies are enabled or not, works for all browsers
   var cookiesEnabledJS = ("cookie" in document && (document.cookie.length > 0 ||
       (document.cookie = "test").indexOf.call(document.cookie, "test") > -1));
   /*  cookies may or may not be working for current page but is it working for console url (:8443) ?
    CookieEnabledCheckFilter redirects here with this param if it's not able to set/retrive cookies - this is done before ajaxswing creates the session/jvm instance.
   */
   var cookiesDisabledParam = "null";
  </SCRIPT>

        <center>

          <div style="width:674px;border:1px solid #DCDCDC">
            <table width="100%" cellpadding="0" cellspacing="0">
              <tr><td align="right" style="background-color:#fdbb30;height:65px;padding-right:10px;" ><img src="/images/symantec.png"></td></tr>
              <tr><td align="left"> </td></tr>
              <tr><td align="left" style="font-family:Arial; font-size:16pt;padding-left:10px;"><b>Symantec Endpoint Protection Manager<br>Web Access</b></td></tr>
            </table>
            <br><br>

            <p align="left" style="padding-left:12px;font-family:Arial, Helvetica, sans-serif; ">You can manage Symantec Endpoint Protection from either of two remote consoles.</p>

            <br><br><br>

            <table cellspacing="0" cellpadding="0" height="96px" width="100%" style="font-family:Arial, Helvetica, sans-serif; font-size: 12px;">
              <tr>
                <td width="322">
                  <table cellspacing="0" cellpadding="0" height="100px" width="322" style="font-family:Arial, Helvetica, sans-serif; font-size: 12px;">
                    <tr>
                      <td align="left" >    </td>
                      <td align="left" style="background-color:#636363">  </td>
                      <SCRIPT LANGUAGE="JavaScript">
         if(cookiesEnabledJS && cookiesDisabledParam == "null") {
        document.write("<td align='left' valign='top' width='100%' style='background-color:#636363'><a style='text-decoration:none; color:white;' href='https://util17-3.enterate.com:8443/console/apps/sepm'><b><br>Symantec Endpoint Protection Manager<br>Web Console<br><br><font color='#FFCC00'>LAUNCH</font></b></a></td>");
        document.write("<td align='left' >    </td>");
         } else {
        document.write("<td align='left' valign='top' width='100%' style='background-color:#636363'><a style='text-decoration:none; color:white;' ><b><br>Symantec Endpoint Protection Manager<br>Web Console<br><br><font color='#FFA500'>You must enable cookies to use the Web Console</font></b></a></td>");
        document.write("<td align='left' >    </td>");
         }
                      </SCRIPT>
                    </tr>
                  </table>
                </td>
                <td width="30"> </td>
                <td width="322">
                  <table cellspacing="0" cellpadding="0" height="100px" width="322" style="font-family:Arial, Helvetica, Verdana, sans-serif; font-size: 12px;">
                    <tr>
                      <td align="left" >    </td>
                      <td align="left" style="background-color:#636363">  </td>
                      <td align="left" valign="top" width="100%" style="background-color:#636363"">
                        <SCRIPT LANGUAGE="JavaScript">
                          if ( javaws18Installed ) {
                            document.write( "<a style='text-decoration:none; color:white;' href='http://util17-3.enterate.com:9090/servlet/JnlpServlet?osSF="+osIs64Bit+"'><b><br>Symantec Endpoint Protection Manager<br>Console<br><br><font color='#FFCC00'>DOWNLOAD & LOG IN</font></b></a>" );
                          } else {
                            document.write( "<a style='text-decoration:none; color:white;' href='http://util17-3.enterate.com:9090/clientpkg/downloadJWS.html'><b><br>Symantec Endpoint Protection Manager<br>Console<br><br><font color='#FFCC00'>DOWNLOAD JAVA 8</font></b></a>" );
                          }
                        </SCRIPT>
                      </td>
                      <td align="left" >    </td>
                    </tr>
                  </table>
                </td>
              </tr>
              <tr>
                <td align="left"  valign="top" style="font-size:12px; padding-left: 10px;padding-top:5px;padding-right:10px;color:#333333;font-family: Arial, Helvetica, sans-serif;"><p align="justify">The Web Console lets you remotely manage Symantec Endpoint Protection in a browser window (requires Internet Explorer 11 (or later), Edge, Firefox, or Chrome).<sup style="color:#d84704;">2</sup></p></td>
                <td> </td>
                <td align="left"  valign="top" style="font-size:12px; padding-left: 10px;padding-top:5px;padding-right:10px;color:#333333;font-family: Arial, Helvetica, sans-serif;"><p align="justify">The remote console lets you remotely manage Symantec Endpoint Protection in a Java client.<sup
```

```
style="color:#d84704;">1,3</sup></p></td>
          </tr>
          <tr>
            <td><br><br><br></td>
            <td>  </td>
            <td>  </td>
          </tr>
          <tr>
            <td width="322">
              <table cellspacing="0" cellpadding="0" height="100px" width="322" style="font-family:Arial, Helvetica, sans-serif; font-size: 12px;">
                <tr>
                  <td align="left">    </td>
                  <td align="left" style="background-color:#636363">  </td>
                  <td align="left" valign="top" width="100%" style="background-color:#636363"><a style="text-decoration:none; color:white"
href="http://util17-3.enterate.com:9090/downloadServerCertificate"><b><br>Symantec Endpoint Protection Manager<br>Certificate<br><br><font
color='#FFCC00'>DOWNLOAD CERTIFICATE</font></b></a></td>
                  <td align="left" >    </td>
                </tr>
              </table>
            </td>
          </tr>
          <tr>
            <td valign="top" align="left" style="font-size:12px; padding-left: 10px;padding-top:5px;padding-right:10px;color:#333333;font-family:
Arial, Helvetica, sans-serif;"><p align="justify">The Symantec Endpoint Protection Manager certificate can be downloaded here.<sup style="color:
#d84704;">2</sup></p></td>
          </tr>
        </table>

        <br><br><br><hr style="display: block;height: 2px;border: 0;background-color:#DCDCDC; margin: 1em 0;padding: 0; "><br><br>

        <table cellspacing="0" cellpadding="0" width="100%" style="font-size:10px; color:#636363;font-family:arial,helvetica,sans-serif;padding-
left:10px;padding-right:10px;"
          <tr><td valign="top">1. </td><td valign="top" width="100%"><p align="justify">On Microsoft Windows Server 2008, and Windows 7, you
must have administrative privileges on the computer where you install the remote console and you must run it using administrative privileges. After
you install the remote console, you can configure the console icon or Start menu item to launch using your administrative privileges. To configure the
Properties, right-click the Symantec Endpoint Protection Manager Console icon on the Windows Desktop or the Symantec Endpoint Protection
Manager Console item on the Start menu, and click Properties > Advanced > Run as Administrator.</p><br><br></td></tr>
          <tr><td valign="top">2. </td><td valign="top" width="100%"><p align="justify">You may receive a certificate warning when you access
the Web Console. You can eliminate this warning by adding the self-signed certificate to your Trusted Root Certification Authorities. For more
information, see <a href='http://entced.symantec.com/entt?product=sep&version=14.0.0000&language=english&module=console&error=
install_cert_trusted_root_ca' target=_new style=color:#d84704;>How to install the certificate for Endpoint Protection Manager Web Console
access.</a></p><br><br></td></tr>
          <tr><td valign="top">3. </td><td valign="top" width="100%"><p align="justify">On 64-bit systems that have installed both 32-bit and 64-
bit versions of Java Runtime Environment (JRE), you must first uninstall the 32-bit version.</p><br><br></td></tr>
          <tr><td valign="top">  </td><td valign="top" width="100%"><p align="justify">For supported browser versions, consult the system
requirements for the version of Symantec Endpoint Protection that you use. See <a href='http://entced.symantec.com/entt?product=
sep&version=14.0.0000&language=english&module=console&error=system_requirements' target=_new style=color:#d84704;>Release notes, new
fixes, and system requirements for all versions of Endpoint Protection.</a></p><br><br></td></tr>
        </table>
        <br><br>

        <p align="left" style="font-size:10px; color:#636363;font-family:arial,helvetica,sans-serif;padding-left:10px;">©1995 - 2019 Symantec
Corporation</p>

      </div>
    </center>
  </body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8443




<!--
SYMANTEC:     Copyright (c) 2019 Symantec Corporation. All rights reserved.

THIS SOFTWARE CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF SYMANTEC CORPORATION.  USE,
DISCLOSURE OR REPRODUCTION IS PROHIBITED WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF SYMANTEC
CORPORATION.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in
FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer
Software - Restricted Rights" and DFARS 227.7202, Rights in "Commercial Computer Software or Commercial
Computer Software Documentation," as applicable, and any successor regulations, whether delivered by
Symantec as on premises or hosted services.  Any use, modification, reproduction release, performance,
display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely
in accordance with the terms of this Agreement.
-->










<html>
    <head>
        <META HTTP-EQUIV="content-type" CONTENT="text/html; charset=UTF-8">
  <!-- VBScript support is removed from IE. Refer following links
    http://msdn.microsoft.com/en-us/library/windows/apps/Hh700404.aspx indicates that support was removed from the ExecScript API. http://msdn.
microsoft.com/en-us/library/ie/dn384057(v=vs.85).aspx explains that it's removed from IE11 Edge mode in the Internet Zone.
    So if we want to run VBScript on IE, we need to add the following to the HEAD tag, this will ensure VBScript ca run on IE.
    e.g. META tag to be added to HEAD tag.
    <META http-equiv="x-ua-compatible" content="IE=10">
  -->
  <META http-equiv="X-UA-Compatible" content="IE=8" >
        <title>Symantec Endpoint Protection Manager</title>

  <SCRIPT LANGUAGE="JavaScript">
   if (top.frames.length > 0) {
    top.location=self.document.location;
   }
  </SCRIPT>

  <!-- First, determine if user agent is IE or Netscape browser -->
  <SCRIPT LANGUAGE="JavaScript">
```

```
   var browserName2 = "Unsupported";
   var browserName = getBrowserName();
   function getBrowserName() {
    var browserNameValue = 'Other';
    var userAgent = navigator.userAgent.toLowerCase();
    if (userAgent.indexOf('edge') >= 0) {
     browserNameValue = 'Edge';
     browserName2 = "Microsoft Edge";
    } else if (userAgent.indexOf('trident') >= 0) {
     browserNameValue = 'MSIE';
     browserName2 =  "Microsoft Internet Explorer";
    } else if (userAgent.indexOf('firefox') >= 0) {
     browserNameValue = 'Firefox';
     browserName2 = "Mozilla Firefox";
    } else if (userAgent.indexOf('chrome') >= 0 && userAgent.indexOf('safari') >= 0 && userAgent.indexOf('webkit') >= 0 && userAgent.indexOf('edge')
== -1 && userAgent.indexOf('opera') == -1 && userAgent.indexOf('opr') == -1) {
     browserNameValue = 'Chrome'
     browserName2 = "Google Chrome";
    } else if (userAgent.indexOf('opera') >= 0 || (userAgent.indexOf('chrome') >= 0 && userAgent.indexOf('safari') >= 0 && userAgent.indexOf('opr') >=
0)) {
     browserNameValue = 'Opera'
     browserName2 = "Opera";
    }
    return browserNameValue;
   }

   var osIs64Bit = is64BitOS();
   function is64BitOS() {
    var userAgent = navigator.userAgent.toLowerCase();
    var is64Bit = (userAgent.indexOf('win64; x64') >= 0 || userAgent.indexOf('wow64') >= 0);
    return is64Bit;
   }

   var browserIs64Bit = is64BitBrowser();
   function is64BitBrowser() {
    var userAgent = navigator.userAgent.toLowerCase();
    var is64Bit = (userAgent.indexOf('win64; x64') >= 0);
    return is64Bit;
   }

   var javaPluginInstalled = isJavaPluginDetected();
   function isJavaPluginDetected() {
    var javaPluginDetected = false;
    if (navigator.mimeTypes) {
     // Why are we not checking navigator.mimeTypes.length here?
     // Answer: Recent 64-bit Firefox browser returns '0' for navigator.mimeTypes.length where as returns
     // 'specific value for navigator.mimeTypes['application/x-java-jnlp-file']. So checking navigator.mimeTypes.length > 0
     // is blocking us from detecting java mime type.
     if (navigator.mimeTypes['application/x-java-jnlp-file'] || navigator.mimeTypes['application/x-java-vm']) {
      javaPluginDetected = true;
     }
    }
    return javaPluginDetected;
   }
  </SCRIPT>

  <SCRIPT LANGUAGE="JavaScript">
            var javaws15Installed=0;
            var javaws16Installed=0;
   var javaws17Installed=0;
   var javaws18Installed=0;
   var isIE = "false";
   if (browserName == "MSIE") {
    isIE = "true";
   }

   if (javaPluginInstalled) {
    javaws15Installed=1;
    javaws16Installed=1;
    javaws17Installed=1;
    javaws18Installed=1;
            }
        </SCRIPT>

        <!-- Now, if it is IE on Windows platform, we check to see which version of JWS is installed -->
        <!-- What happens with the VBScript in non-IE browser? Answer: This block won't get executed -->
        <SCRIPT LANGUAGE="VBScript">
            on error resume next
            If isIE = "true" Then
                    If Not(IsObject(CreateObject("JavaWebStart.isInstalled.1.5.0.0"))) Then
                             javaws15Installed = 0
                    Else
                             javaws15Installed = 1
                    End If
                    If Not(IsObject(CreateObject("JavaWebStart.isInstalled.1.6.0.0"))) Then
                             javaws16Installed = 0
                    Else
                             javaws16Installed = 1
                    End If
     If Not(IsObject(CreateObject("JavaWebStart.isInstalled.1.7.0.0"))) Then
                             javaws17Installed = 0
                    Else
                             javaws17Installed = 1
     End If
     If Not(IsObject(CreateObject("JavaWebStart.isInstalled.1.8.0.0"))) Then
                             javaws18Installed = 0
                    Else
                             javaws18Installed = 1
     End If
            End If
        </SCRIPT>
    </head>

    <body style="font-family: Arial, Helvetica, sans-serif;
                 font-size: 12px;">

        <SCRIPT LANGUAGE="JavaScript">
            if ( javaws18Installed ) {
                document.write('<applet code="com.sygate.scm.server.servlet.JavaVersionCheck" width="1" height="1" archive="scm-version-check.jar"
name="JavaVersionCheck"><param name="permissions" value="all-permissions"/><param name="minimumVersion" value="1.8.0_221"></applet>
');
                try {
                    var sysJava = JavaVersionCheck.isValidVersion();
                    if ( sysJava ) {
                        javaws18Installed = 1;
                    } else {
                        javaws18Installed = 0;
                    }
                } catch( e ) {
                    //alert("DEBUG: Applet execution throws following error: " + e.description);
                    // Applet can be executed if the remote computer has required JRE version installed. If installed JRE
     // is less than the required JRE version we may experience runtime issues such as API not found etc.
                    javaws18Installed = 0;
                }
            }
        </SCRIPT>

  <NOSCRIPT>
      <div style="background-color:#FFCC00;font-size:20pt;text-align:center">
          You must have JavaScript enabled to use this Web page.
      </div>
  </NOSCRIPT>

  <div id="supportedBrowsersMsg" style="background-color:#FDBB30;font-size:16pt;text-align:center;visibility:hidden">
         You are using an older browser version and might experience issues using this browser version to log on to the Web Console. See the
supported browser list under Web Console.
     </div>

  <!-- Web console is only supported on IE7 and later -->
        <SCRIPT LANGUAGE="JavaScript">
     if (isIE == "true") {
   var ix;
      var nAgt = navigator.userAgent;
   var verOffset=nAgt.indexOf("Trident");
   var fullVersion = nAgt.substring(verOffset+8);
   var baseversion;
   if ((ix=fullVersion.indexOf(";"))!=-1) fullVersion=fullVersion.substring(0,ix);

   //get the integer part
   if ((ix=fullVersion.indexOf("."))!=-1) baseversion=fullVersion.substring(0,ix);
   if (parseInt(baseversion) < 7) {
    document.getElementById("supportedBrowsersMsg").style.visibility = "visible";
   }
     }
        </SCRIPT>
        <SCRIPT LANGUAGE="JavaScript">

   // Client-side check if cookies are enabled or not, works for all browsers
   var cookiesEnabledJS = ("cookie" in document && (document.cookie.length > 0 ||
       (document.cookie = "test").indexOf.call(document.cookie, "test") > -1));

   /*  cookies may or may not be working for current page but is it working for console url (:8443) ?
    CookieEnabledCheckFilter redirects here with this param if it's not able to set/retrive cookies - this is done before ajaxswing creates the session/
jvm instance.
   */
   var cookiesDisabledParam = "null";
  </SCRIPT>

        <center>

            <div style="width:674px;border:1px solid #DCDCDC">
                <table width="100%" cellpadding="0" cellspacing="0">
                    <tr><td align="right" style="background-color:#fdbb30;height:65px;padding-right:10px;" ><img src="/images/symantec.png"></td></tr>
                    <tr><td align="left"> </td></tr>
                    <tr><td align="left" style="font-family:Arial; font-size:16pt;padding-left:10px;"><b>Symantec Endpoint Protection Manager<br>Web
Access</b></td></tr>
                </table>
                <br><br>

                <p align="left" style="padding-left:12px;font-family:Arial, Helvetica, sans-serif; ">You can manage Symantec Endpoint Protection from
either of two remote consoles.</p>

                <br><br><br>

                <table cellspacing="0" cellpadding="0" height="96px" width="100%" style="font-family:Arial, Helvetica, sans-serif; font-size: 12px;">
                    <tr>
                        <td width="322">
                            <table cellspacing="0" cellpadding="0" height="100px" width="322" style="font-family:Arial, Helvetica, sans-serif; font-size: 12px;">
                                <tr>
                                    <td align="left" >    </td>
                                    <td align="left" style="background-color:#636363">  </td>
                                    <SCRIPT LANGUAGE="JavaScript">
           if(cookiesEnabledJS && cookiesDisabledParam == "null") {
          document.write("<td align='left' valign='top' width='100%' style='background-color:#636363'><a style='text-decoration:none; color:white;' href=
'https://util17-3.enterate.com:8443/console/apps/sepm'><b><br>Symantec Endpoint Protection Manager<br>Web Console<br><br><font color=
'#FFCC00'>LAUNCH</font></b></a></td>");
          document.write("<td align='left' >    </td>");
           } else {
          document.write("<td align='left' valign='top' width='100%' style='background-color:#636363'><a style='text-decoration:none; color:white;' ><
b><br>Symantec Endpoint Protection Manager<br>Web Console<br><br><font color='#FFA500'>You must enable cookies to use the Web
Console</font></b></a></td>");
          document.write("<td align='left' >    </td>");
           }
                                    </SCRIPT>
                                </tr>
                            </table>
                        </td>
                        <td width="30"> </td>
                        <td width="322">
                            <table cellspacing="0" cellpadding="0" height="100px" width="322" style="font-family:Arial, Helvetica, Verdana, sans-serif; font-
size: 12px;">
                                <tr>
                                    <td align="left" >    </td>
                                    <td align="left" style="background-color:#636363">  </td>
                                    <td align="left" valign="top" width="100%" style="background-color:#636363"">
                                        <SCRIPT LANGUAGE="JavaScript">
                                            if ( javaws18Installed ) {
                                                document.write( "<a style='text-decoration:none; color:white;' href='http://util17-3.enterate.com:9090/servlet/
JnlpServlet?osSF="+osIs64Bit+"'><b><br>Symantec Endpoint Protection Manager<br>Console<br><br><font color='#FFCC00'>DOWNLOAD &
LOG IN</font></b></a>" );
                                            } else {
                                                document.write( "<a style='text-decoration:none; color:white;' href='http://util17-3.enterate.com:9090/clientpkg/
downloadJWS.html'><b><br>Symantec Endpoint Protection Manager<br>Console<br><br><font color='#FFCC00'>DOWNLOAD JAVA 8</font></
b></a>" );
                                            }
                                        </SCRIPT>
                                    </td>
                                    <td align="left" >    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <tr>
                        <td align="left"  valign="top" style="font-size:12px; padding-left: 10px;padding-top:5px;padding-right:10px;color:#333333;font-family: Arial, Helvetica, sans-serif;"><p align="justify">The Web Console lets you remotely manage Symantec Endpoint Protection in a browser window (requires Internet Explorer 11 (or later), Edge, Firefox, or Chrome).<sup style="color:#d84704;">2</sup></p></td>
                        <td> </td>
                        <td align="left"  valign="top" style="font-size:12px; padding-left: 10px;padding-top:5px;padding-right:10px;color:#333333;font-family: Arial, Helvetica, sans-serif;"><p align="justify">The remote console lets you remotely manage Symantec Endpoint Protection in a Java client.<sup style="color:#d84704;">1,3</sup></p></td>
                    </tr>
                    <tr>
                        <td><br><br><br></td>
                        <td>  </td>
                        <td>  </td>
                    </tr>
                    <tr>
                        <td width="322">
                            <table cellspacing="0" cellpadding="0" height="100px" width="322" style="font-family:Arial, Helvetica, sans-serif; font-size: 12px;">
                                <tr>
                                    <td align="left">    </td>
                                    <td align="left" style="background-color:#636363">  </td>
                                    <td align="left" valign="top" width="100%" style="background-color:#636363"><a style="text-decoration:none; color:white" href="http://util17-3.enterate.com:9090/downloadServerCertificate"><b><br>Symantec Endpoint Protection Manager<br>Certificate<br><br><font color='#FFCC00'>DOWNLOAD CERTIFICATE</font></b></a></td>
                                    <td align="left" >    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <tr>
                        <td valign="top" align="left" style="font-size:12px; padding-left: 10px;padding-top:5px;padding-right:10px;color:#333333;font-family: Arial, Helvetica, sans-serif;"><p align="justify">The Symantec Endpoint Protection Manager certificate can be downloaded here.<sup style="color: #d84704;">2</sup></p></td>
                    </tr>
                </table>

                <br><br><br><hr style="display: block;height: 2px;border: 0;background-color:#DCDCDC; margin: 1em 0;padding: 0; "><br><br>

                <table cellspacing="0" cellpadding="0" width="100%" style="font-size:10px; color:#636363;font-family:arial,helvetica,sans-serif;padding-left:10px;padding-right:10px;"
                    <tr><td valign="top">1. </td><td valign="top" width="100%"><p align="justify">On Microsoft Windows Server 2008, and Windows 7, you must have administrative privileges on the computer where you install the remote console and you must run it using administrative privileges. After you install the remote console, you can configure the console icon or Start menu item to launch using your administrative privileges. To configure the Properties, right-click the Symantec Endpoint Protection Manager Console icon on the Windows Desktop or the Symantec Endpoint Protection Manager Console item on the Start menu, and click Properties > Advanced > Run as Administrator.</p><br><br></td></tr>
                    <tr><td valign="top">2. </td><td valign="top" width="100%"><p align="justify">You may receive a certificate warning when you access the Web Console. You can eliminate this warning by adding the self-signed certificate to your Trusted Root Certification Authorities. For more information, see <a href='http://entced.symantec.com/entt?product=sep&version=14.0.0000&language=english&module=console&error=install_cert_trusted_root_ca' target=_new style=color:#d84704;>How to install the certificate for Endpoint Protection Manager Web Console access.</a></p><br><br></td></tr>
                    <tr><td valign="top">3. </td><td valign="top" width="100%"><p align="justify">On 64-bit systems that have installed both 32-bit and 64-bit versions of Java Runtime Environment (JRE), you must first uninstall the 32-bit version.</p><br><br></td></tr>
                    <tr><td valign="top">  </td><td valign="top" width="100%"><p align="justify">For supported browser versions, consult the system requirements for the version of Symantec Endpoint Protection that you use. See <a href='http://entced.symantec.com/entt?product=sep&version=14.0.0000&language=english&module=console&error=system_requirements' target=_new style=color:#d84704;>Release notes, new fixes, and system requirements for all versions of Endpoint Protection.</a></p><br><br></td></tr>
                </table>
                <br><br>

                <p align="left" style="font-size:10px; color:#636363;font-family:arial,helvetica,sans-serif;padding-left:10px;">©1995 - 2019 Symantec Corporation</p>

            </div>
        </center>
    </body>
</html>
```

▮▯▯▯▯ 1 SSL Server Information Retrieval port 8443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-CAMELLIA128-SHA	DH	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
DHE-RSA-CAMELLIA256-SHA	DH	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	brainpoolp512r1	512	yes	256	low
ECDHE	brainpoolp384r1	384	yes	192	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	brainpoolp256r1	256	yes	128	low

ECDHE	secp256k1	256	yes	128	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	sect283r1	283	yes	141	low

1 SSL/TLS Protocol Properties port 8443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 8443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)

(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

1 Web Server Supports HTTP Request Pipelining port 8443/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.10.21:8443

GET /Q_Evasive/ HTTP/1.1
Host:172.17.10.21:8443
```

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:46:01 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:46:06 GMT
Connection: close
Content-Length: 315

   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: util17-3.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:46:01 GMT
```

```
Connection: close
Content-Length: 315
```

1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:48:22 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:48:32 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: util17-3.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:48:22 GMT
Connection: close
Content-Length: 315
```

▮□□□□ 1 Default Web Page port 8446/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8446
```

```
HTTP/1.1 404 Not Found
Content-Length: 0
Date: Sat, 20 Feb 2021 06:02:40 GMT
Connection: keep-alive
Server: SEPM
```

1 Default Web Page (Follow HTTP Redirection) port 8446/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8446


HTTP/1.1 404 Not Found
Content-Length: 0
Date: Sat, 20 Feb 2021 06:03:49 GMT
Connection: keep-alive
Server: SEPM
```

1 SSL Server Information Retrieval port 8446/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-CAMELLIA128-SHA	DH	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
DHE-RSA-CAMELLIA256-SHA	DH	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information — port 8446/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance — port 8446/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8446/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	brainpoolp512r1	512	yes	256	low
ECDHE	brainpoolp384r1	384	yes	192	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	brainpoolp256r1	256	yes	128	low

ECDHE	secp256k1	256	yes	128	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	sect283r1	283	yes	141	low

■□□□□ 1 SSL/TLS Protocol Properties port 8446/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8446/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8446/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 8446/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)

(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

1 Web Server Supports HTTP Request Pipelining port 8446/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.10.21:8446

GET /Q_Evasive/ HTTP/1.1
Host:172.17.10.21:8446



HTTP/1.1 404 Not Found
Content-Length: 0
Date: Sat, 20 Feb 2021 06:14:09 GMT
Server: SEPM

HTTP/1.1 404 Not Found
Content-Length: 0
Date: Sat, 20 Feb 2021 06:14:09 GMT
Server: SEPM
```

1 Default Web Page port 8014/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8014



HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 05:57:54 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 198
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL / was not found on this server.</p>
</body></html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 8014/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8014



HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 05:59:19 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 198
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL / was not found on this server.</p>
</body></html>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 8014/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 8014.

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8014



HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 05:57:54 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 198
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 8014/tcp

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.10.21:8014

GET /Q_Evasive/ HTTP/1.1
Host:172.17.10.21:8014
```

```
HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 06:14:02 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 198
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL / was not found on this server.</p>
</body></html>
HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 06:14:02 GMT
Server: Symantec Endpoint Protection Manager
X-Content-Type-Options: nosniff
Content-Length: 208
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /Q_Evasive/ was not found on this server.</p>
</body></html>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 8446/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8446.

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8446



HTTP/1.1 404 Not Found
Content-Length: 0
Date: Sat, 20 Feb 2021 06:02:40 GMT
Connection: keep-alive
Server: SEPM
```

▮□□□□ 1 HTTP Response Method and Header Information Collected port 8445/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8445.

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8445



HTTP/1.1 302 Found
Date: Sat, 20 Feb 2021 06:05:49 GMT
Server: Symantec Endpoint Protection Manager
Content-Security-Policy: frame-ancestors 'self' util17-3.enterate.com:8443
X-Frame-Options: ALLOW-FROM https://util17-3.enterate.com:8443
X-Content-Type-Options: nosniff
```

```
location: https://util17-3:8445/Reporting/login/NoJavascript.php
Connection: close
Content-Type: text/html; charset=UTF-8
```

1 List of Web Directories port 8445/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/content/	brute force
\	brute force
/Content/	brute force

1 Default Web Page port 8445/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8445
```

1 Default Web Page (Follow HTTP Redirection) port 8445/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: util17-3.enterate.com:8445
```

1 SSL Server Information Retrieval port 8445/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
CAMELLIA128-SHA	RSA	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-CAMELLIA128-SHA	DH	RSA	SHA1	Camellia(128)	MEDIUM
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
CAMELLIA256-SHA	RSA	RSA	SHA1	Camellia(256)	HIGH
DHE-RSA-CAMELLIA256-SHA	DH	RSA	SHA1	Camellia(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8445/tcp over SSL

QID: 38291
Category: General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8445/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8445/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	brainpoolp512r1	512	yes	256	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low

ECDHE	brainpoolp384r1	384	yes	192	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low
ECDHE	brainpoolp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 8445/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8445/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 8445/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8445/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)

(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77

▮□□□□ 1 Web Server Supports HTTP Request Pipelining port 8445/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.10.21:8445

GET /Q_Evasive/ HTTP/1.1
Host:172.17.10.21:8445



HTTP/1.1 302 Found
Date: Sat, 20 Feb 2021 06:14:20 GMT
Server: Symantec Endpoint Protection Manager
Content-Security-Policy: frame-ancestors 'self' 172.17.10.21:8443
X-Frame-Options: ALLOW-FROM https://172.17.10.21:8443
X-Content-Type-Options: nosniff
location: https://172.17.10.21:8445/Reporting/login/NoJavascript.php
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

2


0

HTTP/1.1 404 Not Found
Date: Sat, 20 Feb 2021 06:14:20 GMT
Server: Symantec Endpoint Protection Manager
Content-Security-Policy: frame-ancestors 'self' (null):8443
X-Frame-Options: ALLOW-FROM https://(null):8443
X-Content-Type-Options: nosniff
Content-Length: 208
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /Q_Evasive/ was not found on this server.</p>
</body></html>
```

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH

AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the

target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low

ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:

(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)

(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:

(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

Information Gathered (92)

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: qa-web1.enterate.com
```

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 7239/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:

This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 7239.
GET / HTTP/1.0
Host: qa-web1.enterate.com:7239
```

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2012 R2 Standard	CIFS via TCP Port 445	
Windows 2012 R2/8.1	NTLMSSP	
Windows 2012	TCP/IP Fingerprint	U3423:80
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCOM System Activator	0.0	49154			
Microsoft Local Security Architecture	0.0	49155, 49171			
Microsoft LSA DS Access	0.0	49155, 49171			
Microsoft Network Logon	1.0	49155, 49171			
Microsoft Scheduler Control Service	1.0	49154			
Microsoft Security Account Manager	1.0	49155, 49171			
Microsoft Server Service	3.0	49154			
Microsoft Task Scheduler	1.0	49154			
MS Wbem Transport IEnumWbemClassObject	0.0	49154			
MS Wbem Transport IWbemLevel1Login	0.0	49154			
MS Wbem Transport IWbemObjectSink	0.0	49154			
MS Wbem Transport IWbemServices	0.0	49154			
(Unknown Service)	1.0	49155, 49171			

(Unknown Service)	0.0	49154
(Unknown Service)	1.0	49154
(Unknown Service)	1.0	49152
(Unknown Service)	0.0	49155, 49171
(Unknown Service)	4.0	49154

2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 80, the host's uptime is 8 days, 18 hours, and 49 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Access to Remote Registry Service is denied, error: 0x0

2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1
```

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1
```

2 Microsoft ASP.NET HTTP Handlers Enumerated port 7239/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
.Aspx,.Asmx,.Rem,.Soap,
```

2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 7239/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
.Aspx,.Asmx,.Rem,.Soap,

2 Web Server HTTP Protocol Versions port 7239/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 7239 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 8172/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 8172 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.20.20	qa-web1.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 1, 7, 11.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2512,2514-2701,
2703-3388,3390-5630,5632-5984,5986-6128,6130-7238,7240-8171,8173-40876,
```

40878-42423,42425-47000,47002-49151,49156-49170,49172-49179,49181,49183-65535

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2601 seconds

Start time: Sat, Feb 20 2021, 05:37:08 GMT

End time: Sat, Feb 20 2021, 06:20:29 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
qa-web1.enterate.com	NTLM DNS
qa-web1.enterate.com	FQDN
QA-WEB1	NTLM NetBIOS

■□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:49:53
TCP	135	0:07:38
TCP	443	1:04:14
TCP	445	0:00:01
TCP	3389	0:00:51
TCP	5985	0:28:30
TCP	7239	0:49:38
TCP	8172	0:55:02
TCP	47001	0:32:26
TCP	49152	0:05:12
TCP	49153	0:05:05
TCP	49154	0:05:20
TCP	49155	0:05:05
TCP	49171	0:05:05
TCP	49180	0:05:05
TCP	49182	0:05:05

■□□□□ 1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
7239	unknown	unknown	http over ssl	
8172	unknown	unknown	http over ssl	
47001	unknown	unknown	http	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	
49155	unknown	unknown	msrpc	
49171	unknown	unknown	msrpc	
49180	unknown	unknown	msrpc	
49182	unknown	unknown	msrpc	

■□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:11 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QA-WEB1

■□□□□ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1123089163 with a standard deviation of 676560229. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5176 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many

operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 80: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 21 milli seconds
```

■□□□□ 1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com


<head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a HREF="https://qa-web1.enterate.com/">here</a></body>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

```
GET / HTTP/1.0
Host: qa-web1.enterate.com



HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: https://qa-web1.enterate.com/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:38:28 GMT
Connection: keep-alive
Content-Length: 152
```

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 80/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

■□□□□ 1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/admin/	web page
/help/	web page
/install/	web page
/secure/	web page
/manager/	web page

1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com



HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:46:58 GMT
Connection: keep-alive
Content-Length: 0
```

1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com



HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:49:07 GMT
Connection: keep-alive
Content-Length: 0
```

▮□□□□ 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮▯▯▯▯ 1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 443/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as

the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona

localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale

organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad

(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

1 Web Server Supports HTTP Request Pipelining port 443/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.20.20:443

GET /Q_Evasive/ HTTP/1.1
Host:172.17.20.20:443



HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 06:13:41 GMT
```

```
Content-Length: 0

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 06:13:41 GMT
Content-Length: 0
```

1 HTTP Response Method and Header Information Collected port 443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 443.

```
GET / HTTP/1.0
Host: qa-web1.enterate.com


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:46:58 GMT
Connection: keep-alive
```

Content-Length: 0

1 Referrer-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 443 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

1 List of Web Directories port 443/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/WebID/	brute force
/webid/	brute force

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:17 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:53 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:50:17 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 7239/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 7239/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 7239.

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:7239



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:58:12 GMT
Connection: keep-alive
Content-Length: 701
```

1 Referrer-Policy HTTP Security Header Not Detected port 7239/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 7239 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 7239/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubdomains

■□□□□ 1 Microsoft IIS ASP.NET Version Obtained port 7239/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
X-AspNet-Version: 4.0.30319

■□□□□ 1 List of Web Directories port 7239/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/stats/	brute force

■□□□□ 1 Default Web Page port 7239/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:7239



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:58:12 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
```

```
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 7239/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:7239


HTTP/1.1 200 OK
```

```
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:58:55 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 SSL Server Information Retrieval port 7239/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 7239/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 7239/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 7239/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-

Edited: No
PCI Vuln: No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 7239/tcp over SSL

QID: 38706
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/12/2018
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 7239/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 7239/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 7239/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 7239/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)

(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)

(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b

(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

1 Default Web Page port 8172/tcp over SSL

QID: 12230
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/15/2019
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:8172



HTTP/1.1 404 Not Found
Server: Microsoft-IIS/8.5
Date: Sat, 20 Feb 2021 06:00:48 GMT
Connection: close
Content-Length: 0
```

1 Default Web Page (Follow HTTP Redirection) port 8172/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:8172



HTTP/1.1 404 Not Found
Server: Microsoft-IIS/8.5
Date: Sat, 20 Feb 2021 06:02:38 GMT
Connection: close
Content-Length: 0
```

■□□□□ 1 SSL Server Information Retrieval port 8172/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 8172/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 8172/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 8172/tcp over SSL

QID:	38704

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 8172/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 8172/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information — port 8172/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information — port 8172/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8172/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1

(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13

(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:

(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

■□□□□ 1 HTTP Response Method and Header Information Collected port 8172/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 8172.

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:8172



HTTP/1.1 404 Not Found
Server: Microsoft-IIS/8.5
Date: Sat, 20 Feb 2021 06:00:48 GMT
Connection: close
Content-Length: 0
```

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:04:18 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:04:51 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: qa-web1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:04:18 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance — port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods — port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as

the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona

localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale

organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad

(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.20.21 (qa-app1.enterate.com, QA-APP1) Windows 2012 R2 Standard

Vulnerabilities (1)

■■□□□ 2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication port 4848/tcp

QID:	86729
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/21/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Web server allows form based authentication without disabling the AutoComplete feature for the password field.
Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:

Contact the vendor to have the AutoComplete attribute disabled for the password field in all forms. The AutoComplete attribute should also be disabled for the user ID field.
Developers can add the following attribute to the form or input element: autocomplete="off"
This attribute prevents the browser from prompting the user to save the populated form values for later reuse.
Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera
However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.
Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET /recipe_view.php?intId=char%2839%29%2b%28SELECT HTTP/1.0
Host: qa-app1.enterate.com:4848
```

```
<form method="POST" class="form" name="loginform" action="j_security_check">
        <table role="presentation">
        <tr>
            <td><label for="Login.username" style="font-weight: bold;">User Name:</label></td>
            <td><input type="text" name="j_username" id="Login.username" tabindex="1" value=""></td>
        </tr>
        <tr>
            <td><label for="Login.password" style="font-weight: bold;">Password:</label>
            <td><input type="password" name="j_password" id="Login.password" tabindex="2">
        <tr>
            <td colspan="2" align="center">
                <input type="submit" class="Btn1"
                    value="Login"
                    title="Log In to GlassFish Administration Console" tabindex="3"
                    onmouseover="javascript: if (this.disabled==0) this.className='Btn1Hov'"
                    onmouseout="javascript: if (this.disabled==0) this.className='Btn1'"
                    onblur="javascript: if (this.disabled==0) this.className='Btn1'"
                    onfocus="javascript: if (this.disabled==0) this.className='Btn1Hov'"
                    name="loginButton" id="loginButton">
             <input type="hidden" name="loginButton.DisabledHiddenField" value="true" />
         </td>
     </tr>
     </table>
        </form>
```

```
GET http://172.17.20.21:1/ HTTP/1.0

GET / HTTP/1.0
Host: qa-app1.enterate.com:4848

GET / HTTP/1.1
Host: qa-app1.enterate.com:4848

GET /designs/imm/index.php HTTP/1.0
Host: qa-app1.enterate.com:4848

GET / HTTP/1.0
Host: qa-app1.enterate.com:4848
Cookie : C107373883=/test43429

GET /mob/ HTTP/1.0
Host: qa-app1.enterate.com:4848

GET /thispagedoesnotexistrandomnameQUALYS HTTP/1.0

GET /libs/granite/core/content/login.html?resource=%2F&$$login$$=%24%24login%24%24&j_reason=unknown&j_reason_code=unknown
HTTP/1.0
Host: qa-app1.enterate.com:4848

GET /admin_ui/mas/ent/login.html HTTP/1.0
Host: qa-app1.enterate.com:4848

GET /login.html HTTP/1.0
Host: 172.17.20.21
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: deflate
Cookie: _appwebSessionId_=$COOKIE
Connection: keep-alive

GET /Javascript/login.js HTTP/1.0
Host: qa-app1.enterate.com:4848
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate

GET / HTTP/1.0
Host: qa-app1.enterate.com:4848
User-Agent: QUALYSQID13654/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
Safari/537.36)

GET /login.php HTTP/1.0
Host: qa-app1.enterate.com:4848
```

```
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate

GET /protected/login.do HTTP/1.0
Host: qa-app1.enterate.com:4848
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

Potential Vulnerabilities (1)

■■■□□ 3 Service Stopped Responding port 56443/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:

The service/daemon is vulnerable to a denial of service attack.

SOLUTION:

This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

3 consecutive connection attempts failed after a total number of 7 successful connections.

Information Gathered (111)

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: qa-app1.enterate.com

■■□□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2012 R2 Standard	CIFS via TCP Port 445	
Windows 2012 R2/8.1	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U6483:135
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

■■□□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCOM System Activator	0.0	49154			
Message Queuing - QM2QM V1	1.0	2107, 2105, 49175, 2103			
Message Queuing - QMRT V1	1.0	2107, 2105, 49175, 2103			
Message Queuing - QMRT V2	1.0	2107, 2105, 49175, 2103			

Message Queuing - RemoteRead V1	1.0	2107, 2105, 49175, 2103
Microsoft Local Security Architecture	0.0	49155, 49159
Microsoft LSA DS Access	0.0	49155, 49159
Microsoft Network Logon	1.0	49155, 49159
Microsoft Scheduler Control Service	1.0	49154
Microsoft Security Account Manager	1.0	49155, 49159
Microsoft Server Service	3.0	49154
Microsoft Task Scheduler	1.0	49154
MS Wbem Transport IEnumWbemClassObject	0.0	49154
MS Wbem Transport IWbemLevel1Login	0.0	49154
MS Wbem Transport IWbemObjectSink	0.0	49154
MS Wbem Transport IWbemServices	0.0	49154
(Unknown Service)	1.0	49155, 49159
(Unknown Service)	0.0	2107, 49154, 2105, 49175, 2103
(Unknown Service)	0.0	49154
(Unknown Service)	1.0	2107, 2105, 49175, 2103
(Unknown Service)	1.0	49154
(Unknown Service)	4.0	49154
(Unknown Service)	1.0	49152
(Unknown Service)	0.0	49155, 49159

■■□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 443, the host's uptime is 6 days, 19 hours, and 8 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

2 Microsoft ASP.NET HTTP Handlers Enumerated port 443/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□ 2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 443/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□ 2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

■■□□ 2 Microsoft ASP.NET HTTP Handlers Enumerated port 85/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□ 2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 85/tcp

QID:	12049
Category:	CGI
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Web Server HTTP Protocol Versions port 85/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 85 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.20.21	qa-app1.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-84,86-134,136-442,444,446-1705,1707-1800,1802-1999,2001-2102,2104,2106,
2108-2146,2148-2512,2514-2701,2703-2868,2870-3388,3390-3699,3701-3819,
3821-3919,3921-4847,4849-5630,5632-5984,5986-6128,6130-7675,7677-8079,
8081-8180,8182-8685,8687-16256,16258-42423,42425-47000,47002-49151,49156-49158,
49160-49174,49177,49179-56442,56444-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Scan duration: 2805 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT
```

End time: Sat, Feb 20 2021, 06:23:52 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
qa-app1.enterate.com	NTLM DNS
qa-app1.enterate.com	FQDN
QA-APP1	NTLM NetBIOS

1 Java Remote Method Invocation Detected

QID:	45186
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/23/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Java Remote Method Invocation or Java RMI, is a mechanism that allows one to invoke a method on an object that exists in another address space.
Java RMI is running on target host.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Service name: Java RMI is running on TCP port 8686.

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	85	0:38:59
TCP	135	0:08:48
TCP	443	0:51:56
TCP	445	0:00:02
TCP	3389	0:00:54
TCP	3700	0:00:47
TCP	3820	0:04:32
TCP	3920	0:03:35
TCP	4848	0:20:35
TCP	5985	0:33:40
TCP	7676	0:00:03
TCP	8080	0:11:20
TCP	8181	0:17:47
TCP	8686	0:05:10
TCP	47001	0:31:44
TCP	49152	0:05:16
TCP	49153	0:05:05
TCP	49154	0:05:07
TCP	49155	0:05:05
TCP	49159	0:05:05
TCP	49175	0:05:05
TCP	49176	0:05:05
TCP	49178	0:05:45
TCP	56443	0:04:07

1 Oracle JMS Open Message Queue Detected

QID:	48154
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/16/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Oracle JMS Open Message Queue is running on the remote host.

QID Detection Logic:(Unauthenticated)
This QID gets the Openmq version from the provided banner.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Oracle JMS Open Message Queue Detected on port - 7676

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled

Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:

Vulnerabilities that require authenticated access may not be reported.

SOLUTION:

On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
85	mit-ml-dev	MIT ML Device	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1801	msmq	Microsoft Message Que	Microsoft Message Queue Server	
2103	zephyr-clt	Zephyr serv-hm connection	msrpc	
2105	minipay	MiniPay	msrpc	
2107	unknown	unknown	msrpc	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
3700	portal of doom	portal_of_doom backdoor	GIOP	
3820	unknown	unknown	GIOP over ssl	
3920	unknown	unknown	unknown over ssl	
4848	unknown	unknown	http over ssl	
5985	unknown	unknown	http	
7676	unknown	unknown	OPENMQ	
8080	http-alt	HTTP Alternate (see port 80)	http	
8181	IpSwitch-IMail-WebStatus	IpSwitch-IMail-WebStatus	http over ssl	
8686	unknown	unknown	RMIRegistry over ssl	
47001	unknown	unknown	http	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	
49155	unknown	unknown	msrpc	
49159	unknown	unknown	msrpc	
49175	unknown	unknown	msrpc	
49176	unknown	unknown	msrpc	
49178	unknown	unknown	msrpc	
56443	unknown	unknown	unknown	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:11 GMT

■□□□□ 1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QA-APP1

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1191194685 with a standard deviation of 598077377. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5088 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2
Duration: 25 milli seconds
```

■□□□□ 1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:39:46 GMT
```

```
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:40:55 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security

parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 443/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

▮▯▯▯▯ 1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1

(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2

(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/

(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

▮▯▯▯▯ 1 Default Web Page port 8080/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:8080
```

```
HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1  Java/Oracle Corporation/1.8)
Accept-Ranges: bytes
ETag: W/"4626-1536340331348"
Last-Modified: Fri, 07 Sep 2018 17:12:11 GMT
Content-Type: text/html
Date: Sat, 20 Feb 2021 05:38:03 GMT
Connection: keep-alive
Content-Length: 4626

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 2010, 2014 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
 body{margin-top:0}
 body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
 h1 {font-size:18pt}
 h2 {font-size:14pt}
 h3 {font-size:12pt}
 code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
 li {padding-bottom: 8px}
 p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
 p.copy {text-align: center}
 table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
 th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
 td.insidehead {font-weight:bold; background:white; text-align: left;}
 a {text-decoration:none; color:#3E6B8A}
 a:visited{color:#917E9C}
 a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0" cellspacing="0"
cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993">       <font color="#ffffff"> <b>GlassFish Server</b></font>       </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The document root folder for this
server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a href="http://localhost:4848">go to the
Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a href="http://www.oracle.com/support/premier/index.html">Oracle Premier
Support for Software</a>. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT
investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional technologies and
frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a href="http://wikis.oracle.com/display/GlassFish/
UsageMetrics">GlassFish Server usage</a> that is transmitted by the Update Tool installer as part of the automatic update processes. No
personally identifiable information is collected by this process.</p>
-->
```

```
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a>  page for information about how to join the GlassFish community. The
GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of
the Java&trade; Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see  <var>as-install</var><code>/docs/about.
html</code>, where <var>as-install</var> is the GlassFish Server installation directory.</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a href="http://www.oracle.com/corporate/contact/">Contact</
a>   |
Copyright © 2010, 2014 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p></body></html>
```

1 Default Web Page (Follow HTTP Redirection) port 8080/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:8080



HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1  Java/Oracle Corporation/1.8)
Accept-Ranges: bytes
ETag: W/"4626-1536340331348"
Last-Modified: Fri, 07 Sep 2018 17:12:11 GMT
Content-Type: text/html
Date: Sat, 20 Feb 2021 05:38:03 GMT
Connection: keep-alive
Content-Length: 4626

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.
```

```
Copyright (c) 2010, 2014 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
 body{margin-top:0}
 body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
 h1 {font-size:18pt}
 h2 {font-size:14pt}
 h3 {font-size:12pt}
 code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
 li {padding-bottom: 8px}
 p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
 p.copy {text-align: center}
 table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
 th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
 td.insidehead {font-weight:bold; background:white; text-align: left;}
 a {text-decoration:none; color:#3E6B8A}
 a:visited{color:#917E9C}
 a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0" cellspacing="0" cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993">       <font color="#ffffff"> <b>GlassFish Server</b></font>       </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The document root folder for this server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a href="http://localhost:4848">go to the Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a href="http://www.oracle.com/support/premier/index.html">Oracle Premier Support for Software</a>. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global reach, lifetime support, ecosystem support, and proactive, automated support.</p>
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional technologies and frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a href="http://wikis.oracle.com/display/GlassFish/UsageMetrics">GlassFish Server usage</a> that is transmitted by the Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by this process.</p>
-->
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a>  page for information about how to join the GlassFish community. The GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of the Java&trade; Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see  <var>as-install</var><code>/docs/about.html</code>, where <var>as-install</var> is the GlassFish Server installation directory.</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a href="http://www.oracle.com/corporate/contact/">Contact</a>   |
Copyright © 2010, 2014 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p></body></html>
```

■□□□□ 1 Web Server Version port 8080/tcp

QID: 86000

Category: Web server

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/03/2020
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
GlassFish Server Open Source Edition 4.1	_

■□□□□ 1 HTTP Methods Returned by OPTIONS Request port 443/tcp

QID: 45056
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/16/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 443.

GET / HTTP/1.0
Host: qa-app1.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:39:46 GMT
Connection: keep-alive
Content-Length: 701
```

■□□□□ 1 Referrer-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 443 port.

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

■□□□□ 1 Microsoft IIS ASP.NET Version Obtained port 443/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
X-AspNet-Version: 4.0.30319
```

■□□□□ 1 List of Web Directories port 443/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/aspnet_client/	brute force

1 SSL Server Information Retrieval port 8686/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					

TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮▯▯▯▯ 1 SSL Session Caching Information port 8686/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 8686/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 8686/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 8686/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended.

Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 8686/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 8686/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 8686/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:

(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none

(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:

(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	0 (0x0)
(2)Signature Algorithm	sha256WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."

commonName	Go Daddy Root Certificate Authority - G2
(2)Valid From	Sep 1 00:00:00 2009 GMT
(2)Valid Till	Dec 31 23:59:59 2037 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(2048 bit)
(2)	RSA Public-Key: (2048 bit)
(2)	Modulus:
(2)	00:bf:71:62:08:f1:fa:59:34:f7:1b:c9:18:a3:f7:
(2)	80:49:58:e9:22:83:13:a6:c5:20:43:01:3b:84:f1:
(2)	e6:85:49:9f:27:ea:f6:84:1b:4e:a0:b4:db:70:98:
(2)	c7:32:01:b1:05:3e:07:4e:ee:f4:fa:4f:2f:59:30:
(2)	22:e7:ab:19:56:6b:e2:80:07:fc:f3:16:75:80:39:
(2)	51:7b:e5:f9:35:b6:74:4e:a9:8d:82:13:e4:b6:3f:
(2)	a9:03:83:fa:a2:be:8a:15:6a:7f:de:0b:c3:b6:19:
(2)	14:05:ca:ea:c3:a8:04:94:3b:46:7c:32:0d:f3:00:
(2)	66:22:c8:8d:69:6d:36:8c:11:18:b7:d3:b2:1c:60:
(2)	b4:38:fa:02:8c:ce:d3:dd:46:07:de:0a:3e:eb:5d:
(2)	7c:c8:7c:fb:b0:2b:53:a4:92:62:69:51:25:05:61:
(2)	1a:44:81:8c:2c:a9:43:96:23:df:ac:3a:81:9a:0e:
(2)	29:c5:1c:a9:e9:5d:1e:b6:9e:9e:30:0a:39:ce:f1:
(2)	88:80:fb:4b:5d:cc:32:ec:85:62:43:25:34:02:56:
(2)	27:01:91:b4:3b:70:2a:3f:6e:b1:e8:9c:88:01:7d:
(2)	9f:d4:f9:db:53:6d:60:9d:bf:2c:e7:58:ab:b8:5f:
(2)	46:fc:ce:c4:1b:03:3c:09:eb:49:31:5c:69:46:b3:
(2)	e0:47
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Key Usage	critical
(2)	Certificate Sign, CRL Sign
(2)X509v3 Subject Key Identifier	3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(2)Signature	(256 octets)
(2)	99:db:5d:79:d5:f9:97:59:67:03:61:f1:7e:3b:06:31
(2)	75:2d:a1:20:8e:4f:65:87:b4:f7:a6:9c:bc:d8:e9:2f
(2)	d0:db:5a:ee:cf:74:8c:73:b4:38:42:da:05:7b:f8:02
(2)	75:b8:fd:a5:b1:d7:ae:f6:d7:de:13:cb:53:10:7e:8a
(2)	46:d1:97:fa:b7:2e:2b:11:ab:90:b0:27:80:f9:e8:9f
(2)	5a:e9:37:9f:ab:e4:df:6c:b3:85:17:9d:3d:d9:24:4f
(2)	79:91:35:d6:5f:04:eb:80:83:ab:9a:02:2d:b5:10:f4
(2)	d8:90:c7:04:73:40:ed:72:25:a0:a9:9f:ec:9e:ab:68
(2)	12:99:57:c6:8f:12:3a:09:a4:bd:44:fd:06:15:37:c1
(2)	9b:e4:32:a3:ed:38:e8:d8:64:f3:2c:7e:14:fc:02:ea
(2)	9f:cd:ff:07:68:17:db:22:90:38:2d:7a:8d:d1:54:f1
(2)	69:e3:5f:33:ca:7a:3d:7b:0a:e3:ca:7f:5f:39:e5:e2
(2)	75:ba:c5:76:18:33:ce:2c:f0:2f:4c:ad:f7:b1:e7:ce
(2)	4f:a8:c4:9b:4a:54:06:c5:7f:7d:d5:08:0f:e2:1c:fe
(2)	7e:17:b8:ac:5e:f6:d4:16:b2:43:09:0c:4d:f6:a7:6b
(2)	b4:99:84:65:ca:7a:88:e2:e2:44:be:5c:f7:ea:1c:f5

■□□□□ 1 SSL Server Information Retrieval port 3820/tcp over SSL

QID:	38116
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3820/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 3820/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3820/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	sect409r1	409	yes	204	low

ECDHE	sect409k1	409	yes	204	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3820/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 3820/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3820/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3820/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption

(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:

(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	

countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2

(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	0 (0x0)
(2)Signature Algorithm	sha256WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)Valid From	Sep 1 00:00:00 2009 GMT
(2)Valid Till	Dec 31 23:59:59 2037 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(2048 bit)
(2)	RSA Public-Key: (2048 bit)
(2)	Modulus:
(2)	00:bf:71:62:08:f1:fa:59:34:f7:1b:c9:18:a3:f7:
(2)	80:49:58:e9:22:83:13:a6:c5:20:43:01:3b:84:f1:
(2)	e6:85:49:9f:27:ea:f6:84:1b:4e:a0:b4:db:70:98:
(2)	c7:32:01:b1:05:3e:07:4e:ee:f4:fa:4f:2f:59:30:
(2)	22:e7:ab:19:56:6b:e2:80:07:fc:f3:16:75:80:39:
(2)	51:7b:e5:f9:35:b6:74:4e:a9:8d:82:13:e4:b6:3f:
(2)	a9:03:83:fa:a2:be:8a:15:6a:7f:de:0b:c3:b6:19:
(2)	14:05:ca:ea:c3:a8:04:94:3b:46:7c:32:0d:f3:00:
(2)	66:22:c8:8d:69:6d:36:8c:11:18:b7:d3:b2:1c:60:
(2)	b4:38:fa:02:8c:ce:d3:dd:46:07:de:0a:3e:eb:5d:
(2)	7c:c8:7c:fb:b0:2b:53:a4:92:62:69:51:25:05:61:
(2)	1a:44:81:8c:2c:a9:43:96:23:df:ac:3a:81:9a:0e:
(2)	29:c5:1c:a9:e9:5d:1e:b6:9e:9e:30:0a:39:ce:f1:
(2)	88:80:fb:4b:5d:cc:32:ec:85:62:43:25:34:02:56:
(2)	27:01:91:b4:3b:70:2a:3f:6e:b1:e8:9c:88:01:7d:
(2)	9f:d4:f9:db:53:6d:60:9d:bf:2c:e7:58:ab:b8:5f:
(2)	46:fc:ce:c4:1b:03:3c:09:eb:49:31:5c:69:46:b3:
(2)	e0:47
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Basic Constraints	critical

(2)	CA:TRUE
(2)X509v3 Key Usage	critical
(2)	Certificate Sign, CRL Sign
(2)X509v3 Subject Key Identifier	3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(2)Signature	(256 octets)
(2)	99:db:5d:79:d5:f9:97:59:67:03:61:f1:7e:3b:06:31
(2)	75:2d:a1:20:8e:4f:65:87:b4:f7:a6:9c:bc:d8:e9:2f
(2)	d0:db:5a:ee:cf:74:8c:73:b4:38:42:da:05:7b:f8:02
(2)	75:b8:fd:a5:b1:d7:ae:f6:d7:de:13:cb:53:10:7e:8a
(2)	46:d1:97:fa:b7:2e:2b:11:ab:90:b0:27:80:f9:e8:9f
(2)	5a:e9:37:9f:ab:e4:df:6c:b3:85:17:9d:3d:d9:24:4f
(2)	79:91:35:d6:5f:04:eb:80:83:ab:9a:02:2d:b5:10:f4
(2)	d8:90:c7:04:73:40:ed:72:25:a0:a9:9f:ec:9e:ab:68
(2)	12:99:57:c6:8f:12:3a:09:a4:bd:44:fd:06:15:37:c1
(2)	9b:e4:32:a3:ed:38:e8:d8:64:f3:2c:7e:14:fc:02:ea
(2)	9f:cd:ff:07:68:17:db:22:90:38:2d:7a:8d:d1:54:f1
(2)	69:e3:5f:33:ca:7a:3d:7b:0a:e3:ca:7f:5f:39:e5:e2
(2)	75:ba:c5:76:18:33:ce:2c:f0:2f:4c:ad:f7:b1:e7:ce
(2)	4f:a8:c4:9b:4a:54:06:c5:7f:7d:d5:08:0f:e2:1c:fe
(2)	7e:17:b8:ac:5e:f6:d4:16:b2:43:09:0c:4d:f6:a7:6b
(2)	b4:99:84:65:ca:7a:88:e2:e2:44:be:5c:f7:ea:1c:f5

■□□□□ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:5985
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:44:41 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:44:45 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:44:41 GMT
Connection: close
Content-Length: 315
```

1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:47:22 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:47:26 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:47001
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:47:22 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 85/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:85



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:50:43 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
```

```
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 85/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:85
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:52:05 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

1 HTTP Methods Returned by OPTIONS Request port 85/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 85/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 85.

GET / HTTP/1.0
Host: qa-app1.enterate.com:85


HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 12 Sep 2018 22:35:58 GMT
Accept-Ranges: bytes
ETag: "1bb3aaf9e84ad41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
```

```
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:50:43 GMT
Connection: keep-alive
Content-Length: 701
```

1 Referrer-Policy HTTP Security Header Not Detected port 85/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Referrer-Policy HTTP Header missing on 85 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 85/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

■□□□□ 1 Microsoft IIS ASP.NET Version Obtained port 85/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
X-AspNet-Version: 4.0.30319
```

■□□□□ 1 List of Web Directories port 85/tcp

QID:	86672

Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/aspnet_client/	brute force

▮▯▯▯▯ 1 SSL Web Server Version port 4848/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/14/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner

1 List of Web Directories port 4848/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/theme/	web page
/theme/com/	web page
/theme/com/sun/	web page
/theme/com/sun/webui/	web page
/theme/com/sun/webui/jsf/	web page
/theme/com/sun/webui/jsf/suntheme/	web page
/theme/com/sun/webui/jsf/suntheme/css/	web page
/resource/	web page
/resource/css/	web page
/theme/META-INF/	web page
/theme/META-INF/dojo/	web page
/theme/META-INF/json/	web page
/theme/META-INF/prototype/	web page
/resource/community-theme/	web page
/resource/community-theme/images/	web page
/resource/js/	web page

1 Default Web Page port 8181/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:8181



HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1  Java/Oracle Corporation/1.8)
Accept-Ranges: bytes
ETag: W/"4626-1536340331348"
Last-Modified: Fri, 07 Sep 2018 17:12:11 GMT
Content-Type: text/html
Date: Sat, 20 Feb 2021 05:57:08 GMT
Connection: keep-alive
Content-Length: 4626

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 2010, 2014 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
 body{margin-top:0}
 body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
 h1 {font-size:18pt}
 h2 {font-size:14pt}
 h3 {font-size:12pt}
 code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
 li {padding-bottom: 8px}
 p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
 p.copy {text-align: center}
 table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
 th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
 td.insidehead {font-weight:bold; background:white; text-align: left;}
 a {text-decoration:none; color:#3E6B8A}
 a:visited{color:#917E9C}
 a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0" cellspacing="0"
cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993">       <font color="#ffffff"> <b>GlassFish Server</b></font>       </td></tr>
```

```
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The document root folder for this
server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a href="http://localhost:4848">go to the
Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a href="http://www.oracle.com/support/premier/index.html">Oracle Premier
Support for Software</a>. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT
investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional technologies and
frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a href="http://wikis.oracle.com/display/GlassFish/
UsageMetrics">GlassFish Server usage</a> that is transmitted by the Update Tool installer as part of the automatic update processes. No
personally identifiable information is collected by this process.</p>
-->
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a>  page for information about how to join the GlassFish community. The
GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of
the Java&trade; Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see  <var>as-install</var><code>/docs/about.
html</code>, where <var>as-install</var> is the GlassFish Server installation directory.</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a href="http://www.oracle.com/corporate/contact/">Contact</
a>   |
Copyright © 2010, 2014 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p></body></html>
```

▮▯▯▯▯ 1 Default Web Page (Follow HTTP Redirection) port 8181/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:8181



HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1  Java/Oracle Corporation/1.8)
Accept-Ranges: bytes
ETag: W/"4626-1536340331348"
Last-Modified: Fri, 07 Sep 2018 17:12:11 GMT
Content-Type: text/html
Date: Sat, 20 Feb 2021 05:57:08 GMT
Connection: keep-alive
Content-Length: 4626

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 2010, 2014 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
 body{margin-top:0}
 body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
 h1 {font-size:18pt}
 h2 {font-size:14pt}
 h3 {font-size:12pt}
 code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
 li {padding-bottom: 8px}
 p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
 p.copy {text-align: center}
 table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
 th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
 td.insidehead {font-weight:bold; background:white; text-align: left;}
 a {text-decoration:none; color:#3E6B8A}
 a:visited{color:#917E9C}
 a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0" cellspacing="0"
cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993">       <font color="#ffffff"> <b>GlassFish Server</b></font>       </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The document root folder for this
server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a href="http://localhost:4848">go to the
Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a href="http://www.oracle.com/support/premier/index.html">Oracle Premier
Support for Software</a>. Premier Support helps lower the total cost and risk of owning your Oracle solutions, improve the return from your IT
investment, and optimize the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional technologies and
frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
```

```
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a href="http://wikis.oracle.com/display/GlassFish/
UsageMetrics">GlassFish Server usage</a> that is transmitted by the Update Tool installer as part of the automatic update processes. No
personally identifiable information is collected by this process.</p>
-->
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a>  page for information about how to join the GlassFish community. The
GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of
the Java&trade; Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see  <var>as-install</var><code>/docs/about.
html</code>, where <var>as-install</var> is the GlassFish Server installation directory.</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a href="http://www.oracle.com/corporate/contact/">Contact</
a>   |
Copyright © 2010, 2014 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p></body></html>
```

1 SSL Server Information Retrieval port 8181/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					

TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 8181/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance — port 8181/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods — port 8181/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low

▮▯▯▯▯ 1 SSL/TLS Protocol Properties port 8181/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

1 SSL Certificate Transparency Information port 8181/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control			

		Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

▮▯▯▯▯ 1 TLS Secure Renegotiation Extension Support Information port 8181/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

▮▯▯▯▯ 1 SSL Certificate - Information port 8181/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95

(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)

(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:

(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	0 (0x0)
(2)Signature Algorithm	sha256WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)Valid From	Sep 1 00:00:00 2009 GMT
(2)Valid Till	Dec 31 23:59:59 2037 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(2048 bit)
(2)	RSA Public-Key: (2048 bit)
(2)	Modulus:

(2)	00:bf:71:62:08:f1:fa:59:34:f7:1b:c9:18:a3:f7:
(2)	80:49:58:e9:22:83:13:a6:c5:20:43:01:3b:84:f1:
(2)	e6:85:49:9f:27:ea:f6:84:1b:4e:a0:b4:db:70:98:
(2)	c7:32:01:b1:05:3e:07:4e:ee:f4:fa:4f:2f:59:30:
(2)	22:e7:ab:19:56:6b:e2:80:07:fc:f3:16:75:80:39:
(2)	51:7b:e5:f9:35:b6:74:4e:a9:8d:82:13:e4:b6:3f:
(2)	a9:03:83:fa:a2:be:8a:15:6a:7f:de:0b:c3:b6:19:
(2)	14:05:ca:ea:c3:a8:04:94:3b:46:7c:32:0d:f3:00:
(2)	66:22:c8:8d:69:6d:36:8c:11:18:b7:d3:b2:1c:60:
(2)	b4:38:fa:02:8c:ce:d3:dd:46:07:de:0a:3e:eb:5d:
(2)	7c:c8:7c:fb:b0:2b:53:a4:92:62:69:51:25:05:61:
(2)	1a:44:81:8c:2c:a9:43:96:23:df:ac:3a:81:9a:0e:
(2)	29:c5:1c:a9:e9:5d:1e:b6:9e:9e:30:0a:39:ce:f1:
(2)	88:80:fb:4b:5d:cc:32:ec:85:62:43:25:34:02:56:
(2)	27:01:91:b4:3b:70:2a:3f:6e:b1:e8:9c:88:01:7d:
(2)	9f:d4:f9:db:53:6d:60:9d:bf:2c:e7:58:ab:b8:5f:
(2)	46:fc:ce:c4:1b:03:3c:09:eb:49:31:5c:69:46:b3:
(2)	e0:47
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Key Usage	critical
(2)	Certificate Sign, CRL Sign
(2)X509v3 Subject Key Identifier	3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(2)Signature	(256 octets)
(2)	99:db:5d:79:d5:f9:97:59:67:03:61:f1:7e:3b:06:31
(2)	75:2d:a1:20:8e:4f:65:87:b4:f7:a6:9c:bc:d8:e9:2f
(2)	d0:db:5a:ee:cf:74:8c:73:b4:38:42:da:05:7b:f8:02
(2)	75:b8:fd:a5:b1:d7:ae:f6:d7:de:13:cb:53:10:7e:8a
(2)	46:d1:97:fa:b7:2e:2b:11:ab:90:b0:27:80:f9:e8:9f
(2)	5a:e9:37:9f:ab:e4:df:6c:b3:85:17:9d:3d:d9:24:4f
(2)	79:91:35:d6:5f:04:eb:80:83:ab:9a:02:2d:b5:10:f4
(2)	d8:90:c7:04:73:40:ed:72:25:a0:a9:9f:ec:9e:ab:68
(2)	12:99:57:c6:8f:12:3a:09:a4:bd:44:fd:06:15:37:c1
(2)	9b:e4:32:a3:ed:38:e8:d8:64:f3:2c:7e:14:fc:02:ea
(2)	9f:cd:ff:07:68:17:db:22:90:38:2d:7a:8d:d1:54:f1
(2)	69:e3:5f:33:ca:7a:3d:7b:0a:e3:ca:7f:5f:39:e5:e2
(2)	75:ba:c5:76:18:33:ce:2c:f0:2f:4c:ad:f7:b1:e7:ce
(2)	4f:a8:c4:9b:4a:54:06:c5:7f:7d:d5:08:0f:e2:1c:fe
(2)	7e:17:b8:ac:5e:f6:d4:16:b2:43:09:0c:4d:f6:a7:6b
(2)	b4:99:84:65:ca:7a:88:e2:e2:44:be:5c:f7:ea:1c:f5

▮▯▯▯▯ 1 Default Web Page port 4848/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:4848




<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
    <title>Login</title>
<script type="text/javascript">
<!-- FIXME: add code to ensure we're the top-most frame -->
    if (document.getElementById('layout-doc') != null) {
        // Just refresh the page... login will take over
        window.location = window.location;
    }
</script>
    <style type="text/css">
        /* clickjacking defense */
        body { display : none; }
    </style>
<link rel="stylesheet" type="text/css" href="/theme/com/sun/webui/jsf/suntheme/css/css_master.css" />
<script type="text/javascript">
djConfig={
    "isDebug": false,
    "debugAtAllCosts": false,
    "parseWidgets": false
};
</script>
<script type="text/javascript" src="/theme/META-INF/dojo/dojo.js"></script>
<script type="text/javascript" src="/theme/META-INF/json/json.js"></script>
<script type="text/javascript" src="/theme/META-INF/prototype/prototype.js"></script>
<script type="text/javascript" src="/theme/META-INF/com_sun_faces_ajax.js"></script>
<script type="text/javascript">
dojo.hostenv.setModulePrefix("webui.suntheme", "/theme/com/sun/webui/jsf/suntheme/javascript");
dojo.require('webui.suntheme.*');
</script>
<link id="sun_link5" rel="stylesheet" type="text/css" href="/resource/css/css_ns6up.css" />

</head>

<body id="body3" class="LogBdy" focus="loginform.j_username" style="background-color: #FFFFFF;">
    <div id="header"class="LogTopBnd" style="background: url('/theme/com/sun/webui/jsf/suntheme/images/login/gradlogtop.jpg') repeat-x; height: 30px;"></div>
    <div class="middle" style="background-image: url(/theme/com/sun/webui/jsf/suntheme/images/login/gradlogsides.jpg);background-repeat:repeat-x;background-position:left top; background-color: #D4DCE1;">
        <div class="plugincontent" style="width1: 1px; visibility: visible;">

<div style="height: 435px;background-image: url(/resource/community-theme/images/login-backimage-open.png);
    background-repeat:no-repeat;background-position:left top; width: 720px; margin: auto;">
    <div style="width: 460px; padding-top: 160px; margin-left: 310px;">
```

```
<img id="sun_image11" src="/resource/community-theme/images/login-product_name_open.png;jsessionid=e037138c1472a2695da6b2598a59"
alt="GlassFish Server Open Source Edition" height="42" width="329" border="0" />
    <form method="POST" class="form" name="loginform" action="j_security_check">
    <table role="presentation">
    <tr>
      <td><label for="Login.username" style="font-weight: bold;">User Name:</label></td>
      <td><input type="text" name="j_username" id="Login.username" tabindex="1" value=""></td>
    </tr>
    <tr>
      <td><label for="Login.password" style="font-weight: bold;">Password:</label>
      <td><input type="password" name="j_password" id="Login.password" tabindex="2">
    <tr>
      <td colspan="2" align="center">
        <input type="submit" class="Btn1"
          value="Login"
          title="Log In to GlassFish Administration Console" tabindex="3"
          onmouseover="javascript: if (this.disabled==0) this.className='Btn1Hov'"
          onmouseout="javascript: if (this.disabled==0) this.className='Btn1'"
          onblur="javascript: if (this.disabled==0) this.className='Btn1'"
          onfocus="javascript: if (this.disabled==0) this.className='Btn1Hov'"
          name="loginButton" id="loginButton">
       <input type="hidden" name="loginButton.DisabledHiddenField" value="true" />
     </td>
   </tr>
   </table>
    </form>
  </div>
</div>

      <script type="text/javascript">
        if (false) {
          //submitAndDisable(document.getElementById('loginButton'), 'Login');
          document.getElementById('loginButton').form.submit();
          //document.getElementById('loginButton').form.autocomplete="off";
        }
      </script>
    </div>
  </div>
  <div class="footer"
    style="background-image: url(/theme/com/sun/webui/jsf/suntheme/images/login/gradlogbot.jpg);background-repeat:repeat-x;background-
position:left top; color: #FFFFFF; background-color: #4A5C68">
    <div id="copyright" style="width: 720px; margin-left: auto; margin-right: auto; padding: 5px;">
      <span>Copyright  2005, 2014, Oracle and/or its affiliates. All rights reserved.  Oracle and Java are registered trademarks of Oracle and/or its
affiliates. Other names may be trademarks of their respective owners.</span>
    </div>
  </div>
  <script src="/resource/js/cj.js"></script>
</body>
</html>
```

▮▯▯▯▯ 1 Default Web Page (Follow HTTP Redirection) port 4848/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-app1.enterate.com:4848




<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
    <title>Login</title>
<script type="text/javascript">
<!-- FIXME: add code to ensure we're the top-most frame -->
    if (document.getElementById('layout-doc') != null) {
        // Just refresh the page... login will take over
        window.location = window.location;
    }
</script>
    <style type="text/css">
        /* clickjacking defense */
        body { display : none; }
    </style>
<link rel="stylesheet" type="text/css" href="/theme/com/sun/webui/jsf/suntheme/css/css_master.css" />
<script type="text/javascript">
djConfig={
    "isDebug": false,
    "debugAtAllCosts": false,
    "parseWidgets": false
};
</script>
<script type="text/javascript" src="/theme/META-INF/dojo/dojo.js"></script>
<script type="text/javascript" src="/theme/META-INF/json/json.js"></script>
<script type="text/javascript" src="/theme/META-INF/prototype/prototype.js"></script>
<script type="text/javascript" src="/theme/META-INF/com_sun_faces_ajax.js"></script>
<script type="text/javascript">
dojo.hostenv.setModulePrefix("webui.suntheme", "/theme/com/sun/webui/jsf/suntheme/javascript");
dojo.require('webui.suntheme.*');
</script>
<link id="sun_link5" rel="stylesheet" type="text/css" href="/resource/css/css_ns6up.css" />

</head>

<body id="body3" class="LogBdy" focus="loginform.j_username" style="background-color: #FFFFFF;">
    <div id="header"class="LogTopBnd" style="background: url('/theme/com/sun/webui/jsf/suntheme/images/login/gradlogtop.jpg') repeat-x; height: 30px;"></div>
    <div class="middle" style="background-image: url(/theme/com/sun/webui/jsf/suntheme/images/login/gradlogsides.jpg);background-repeat:repeat-x;background-position:left top; background-color: #D4DCE1;">
        <div class="plugincontent" style="width1: 1px; visibility: visible;">

<div style="height: 435px;background-image: url(/resource/community-theme/images/login-backimage-open.png);
    background-repeat:no-repeat;background-position:left top; width: 720px; margin: auto;">
    <div style="width: 460px; padding-top: 160px; margin-left: 310px;">
<img id="sun_image11" src="/resource/community-theme/images/login-product_name_open.png;jsessionid=e0371a8159b2a7248f662c42eb60" alt="GlassFish Server Open Source Edition" height="42" width="329" border="0" />
        <form method="POST" class="form" name="loginform" action="j_security_check">
        <table role="presentation">
        <tr>
            <td><label for="Login.username" style="font-weight: bold;">User Name:</label></td>
            <td><input type="text" name="j_username" id="Login.username" tabindex="1" value=""></td>
        </tr>
        <tr>
```

```
            <td><label for="Login.password" style="font-weight: bold;">Password:</label>
            <td><input type="password" name="j_password" id="Login.password" tabindex="2">
        <tr>
            <td colspan="2" align="center">
                <input type="submit" class="Btn1"
                    value="Login"
                    title="Log In to GlassFish Administration Console" tabindex="3"
                    onmouseover="javascript: if (this.disabled==0) this.className='Btn1Hov'"
                    onmouseout="javascript: if (this.disabled==0) this.className='Btn1'"
                    onblur="javascript: if (this.disabled==0) this.className='Btn1'"
                    onfocus="javascript: if (this.disabled==0) this.className='Btn1Hov'"
                    name="loginButton" id="loginButton">
             <input type="hidden" name="loginButton.DisabledHiddenField" value="true" />
         </td>
     </tr>
     </table>
        </form>
    </div>
</div>

            <script type="text/javascript">
                if (false) {
                    //submitAndDisable(document.getElementById('loginButton'), 'Login');
                    document.getElementById('loginButton').form.submit();
                    //document.getElementById('loginButton').form.autocomplete="off";
                }
            </script>
        </div>
    </div>
    <div class="footer"
        style="background-image: url(/theme/com/sun/webui/jsf/suntheme/images/login/gradlogbot.jpg);background-repeat:repeat-x;background-
position:left top; color: #FFFFFF; background-color: #4A5C68">
        <div id="copyright" style="width: 720px; margin-left: auto; margin-right: auto; padding: 5px;">
            <span>Copyright  2005, 2014, Oracle and/or its affiliates. All rights reserved.  Oracle and Java are registered trademarks of Oracle and/or its
affiliates. Other names may be trademarks of their respective owners.</span>
        </div>
    </div>
    <script src="/resource/js/cj.js"></script>
</body>
</html>
```

■□□□□ 1 SSL Server Information Retrieval port 4848/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 4848/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance — port 4848/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods — port 4848/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
DHE		1024	yes	80	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	sect571r1	571	yes	285	low
ECDHE	sect571k1	571	yes	285	low
ECDHE	sect409r1	409	yes	204	low
ECDHE	sect409k1	409	yes	204	low
ECDHE	sect283r1	283	yes	141	low
ECDHE	sect283k1	283	yes	141	low
ECDHE	secp256k1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 4848/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:

Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 4848/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 4848/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 4848/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:

(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:

(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:

(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01
(2)CERTIFICATE 2	
(2)Version	3 (0x2)
(2)Serial Number	0 (0x0)
(2)Signature Algorithm	sha256WithRSAEncryption
(2)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2

(2)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(2)Valid From	Sep 1 00:00:00 2009 GMT
(2)Valid Till	Dec 31 23:59:59 2037 GMT
(2)Public Key Algorithm	rsaEncryption
(2)RSA Public Key	(2048 bit)
(2)	RSA Public-Key: (2048 bit)
(2)	Modulus:
(2)	00:bf:71:62:08:f1:fa:59:34:f7:1b:c9:18:a3:f7:
(2)	80:49:58:e9:22:83:13:a6:c5:20:43:01:3b:84:f1:
(2)	e6:85:49:9f:27:ea:f6:84:1b:4e:a0:b4:db:70:98:
(2)	c7:32:01:b1:05:3e:07:4e:ee:f4:fa:4f:2f:59:30:
(2)	22:e7:ab:19:56:6b:e2:80:07:fc:f3:16:75:80:39:
(2)	51:7b:e5:f9:35:b6:74:4e:a9:8d:82:13:e4:b6:3f:
(2)	a9:03:83:fa:a2:be:8a:15:6a:7f:de:0b:c3:b6:19:
(2)	14:05:ca:ea:c3:a8:04:94:3b:46:7c:32:0d:f3:00:
(2)	66:22:c8:8d:69:6d:36:8c:11:18:b7:d3:b2:1c:60:
(2)	b4:38:fa:02:8c:ce:d3:dd:46:07:de:0a:3e:eb:5d:
(2)	7c:c8:7c:fb:b0:2b:53:a4:92:62:69:51:25:05:61:
(2)	1a:44:81:8c:2c:a9:43:96:23:df:ac:3a:81:9a:0e:
(2)	29:c5:1c:a9:e9:5d:1e:b6:9e:9e:30:0a:39:ce:f1:
(2)	88:80:fb:4b:5d:cc:32:ec:85:62:43:25:34:02:56:
(2)	27:01:91:b4:3b:70:2a:3f:6e:b1:e8:9c:88:01:7d:
(2)	9f:d4:f9:db:53:6d:60:9d:bf:2c:e7:58:ab:b8:5f:
(2)	46:fc:ce:c4:1b:03:3c:09:eb:49:31:5c:69:46:b3:
(2)	e0:47
(2)	Exponent: 65537 (0x10001)
(2)X509v3 EXTENSIONS	
(2)X509v3 Basic Constraints	critical
(2)	CA:TRUE
(2)X509v3 Key Usage	critical
(2)	Certificate Sign, CRL Sign
(2)X509v3 Subject Key Identifier	3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(2)Signature	(256 octets)
(2)	99:db:5d:79:d5:f9:97:59:67:03:61:f1:7e:3b:06:31
(2)	75:2d:a1:20:8e:4f:65:87:b4:f7:a6:9c:bc:d8:e9:2f
(2)	d0:db:5a:ee:cf:74:8c:73:b4:38:42:da:05:7b:f8:02
(2)	75:b8:fd:a5:b1:d7:ae:f6:d7:de:13:cb:53:10:7e:8a
(2)	46:d1:97:fa:b7:2e:2b:11:ab:90:b0:27:80:f9:e8:9f
(2)	5a:e9:37:9f:ab:e4:df:6c:b3:85:17:9d:3d:d9:24:4f
(2)	79:91:35:d6:5f:04:eb:80:83:ab:9a:02:2d:b5:10:f4
(2)	d8:90:c7:04:73:40:ed:72:25:a0:a9:9f:ec:9e:ab:68
(2)	12:99:57:c6:8f:12:3a:09:a4:bd:44:fd:06:15:37:c1
(2)	9b:e4:32:a3:ed:38:e8:d8:64:f3:2c:7e:14:fc:02:ea
(2)	9f:cd:ff:07:68:17:db:22:90:38:2d:7a:8d:d1:54:f1
(2)	69:e3:5f:33:ca:7a:3d:7b:0a:e3:ca:7f:5f:39:e5:e2
(2)	75:ba:c5:76:18:33:ce:2c:f0:2f:4c:ad:f7:b1:e7:ce
(2)	4f:a8:c4:9b:4a:54:06:c5:7f:7d:d5:08:0f:e2:1c:fe
(2)	7e:17:b8:ac:5e:f6:d4:16:b2:43:09:0c:4d:f6:a7:6b
(2)	b4:99:84:65:ca:7a:88:e2:e2:44:be:5c:f7:ea:1c:f5

1 SSL Web Server Version port 8181/tcp

QID:	86001
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/14/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
GlassFish Server Open Source Edition 4.1	_

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

▮▯▯▯▯ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

▮▯▯▯▯ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption

(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:

(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	

countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2

(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.20.22 (qa-db1.enterate.com, QA-DB1) Windows 2016/2019/10

Potential Vulnerabilities (2)

■■■■□ 4 Multiple MS-SQL-7 threats - (I)

QID:	19058
Category:	Database
CVE ID:	CVE-2000-1081, CVE-2001-0542, CVE-2002-0056, CVE-2002-0154
Vendor Reference:	-
Bugtraq ID:	2030, 3733, 4135
Service Modified:	11/13/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

We can remotely detect the presence of Microsoft's SQL Server, but cannot remotely detect if a patch or service pack has already been applied. Verify that you have applied the appropriate patch and/or service pack.
Note: This would appear as a potential for MSSQL versions 9 and above for an unauthenticated scan. MSSQL versions 9 and above are not vulnerable for these issues.
The following threats are present in MS-SQL-7:
1) Microsoft SQL Server/Data Engine various xp_ Buffer Overflow Vulnerabilities. The API Srv_paraminfo() function is implemented by Extended Stored Procedures (XPs). XPs are DLL files that perform high-level functions. When called, they invoke a function called Srv_paraminfo(), which parses the input parameters. Srv_paraminfo() does not check the length of the parameter string that an XP passes to it. The following XPs are affected: xp_displayparamstmt, xp_enumresultset, xp_showcolv, xp_updatecolvbm, xp_peekqueue, xp_printstatements, xp_proxiedmetadata and xp_SetSQLSecurity.
2) Microsoft SQL Server Multiple Overflow and Format String Vulnerabilities
. SQL Server provides built-in functions for the formatting of error messages based on C-style format specifiers. These built-in functions are accessible to all users. Providing maliciously crafted input to these functions results in exploitable error conditions in the SQL Server process. To mount this attack, the malicious user must have permission to execute SQL queries either directly or by leveraging SQL Command Injection flaws.
3) Microsoft SQL Server Provider Name Buffer Overflow Vulnerability
. SQL Server does not perform proper bounds checking of the provider arguments to the OpenDataSource and OpenRowset functions. These functions may be used by an ordinary user to reference OLE DB data sources. As a result, it is possible to cause a buffer overflow condition to occur by providing an excessively long string as a provider name in a query.
4) Microsoft SQL Server xp_dirtree Buffer Overflow Vulnerability
. A vulnerability has been reported in the xp_dirtree function. If an extremely large parameter is passed to the stored procedure xp_dirtree, a buffer overflow condition will occur. This issue may be related to an older known problem with unsafe usage of the Srv_paraminfo() function call.
5) Microsoft SQL Server Administrator Cached Connection Vulnerability
. Query methods are SQL Server commands used to request information from the database. A flaw exists in the handling of specially structured ad hoc queries, which could enable a normal user to gain administrative privileges. In order to gain access to information in the database, a user must make a connection to the server. Once access to the database is no longer required, the user logging off will terminate the connection. However, by design, SQL Server will store the connection used by the user in cache for a certain amount of time. This is done to improve the server's performance. Next time that particular user logs in, SQL Server can reinstate the cached connection rather than creating a new one.
6) Microsoft SQL Server 7.0 NULL Data DoS Vulnerability. SQL Server will crash if it receives a TDS header with three or more NULL bytes as data. The crash will generate an event in the log with ID 17055 "fatal exception EXCEPTION_ACCESS VIOLATION".
7) Microsoft SQL Server 7.0 Stored Procedure Vulnerability. It is possible for users without the proper permissions to run stored procedure code. This includes a full range of tasks, such as modifying, viewing, or deleting entries in the database. This can be accomplished by executing a stored

procedure owned by the SA account, which is referenced from a temporary stored procedure. SQL Server does not properly check the execute permissions on stored procedures referenced by temporary stored procedures.

IMPACT:

1) This vulnerability can only be exploited by users who can successfully log on to the SQL server. By exploiting this vulnerability, it may be possible for malicious users to execute arbitrary code on the host running a vulnerable version of SQL Server. The malicious user would need to overwrite the return address of the calling function with the address of attacker-supplied shell code in memory. This shell code would be executed under the context of the account that the SQL Server service was configured to run under. The account must have a minimum of SYSTEM privileges.
2) By exploiting this vulnerability, it may be possible for malicious users to execute arbitrary code on a host running a vulnerable version of Microsoft's SQL Server.
3) Successful exploitation of this vulnerability could allow a malicious user to execute arbitrary code with the privileges of the database. There is a possibility that this issue may be exploited remotely, either via distributed SQL queries or potentially via an SQL injection attack.
4) If an extremely large parameter is passed to a vulnerable stored procedure, a buffer overflow condition will occur. Depending on the data supplied, this may cause a denial of service condition, or result in the execution of arbitrary code as the SQL Server process.
5) By exploiting this vulnerability, logged-in users can gain administrative privileges to the database.
6) If this vulnerability is exploited, the SQL server will crash.
7) Users must be authenticated on the SQL server and have access to the referring database in order to perform this exploit. By exploiting this vulnerability, it's possible for users without the proper permissions to run database stored procedure code.

SOLUTION:

1) Read Microsoft Security Bulletin MS00-092: Frequently Asked Questions (http://www.microsoft.com/technet/security/bulletin/MS00-092.mspx) for more information about this vulnerability and for instructions on how to download and install the patches.
2) Read Microsoft Security Bulletin MS01-060 (http://www.microsoft.com/technet/security/bulletin/MS01-060.mspx) for more information about this vulnerability and for instructions on how to download and install the patches.
3,4,5,6,7) Update to Microsoft SQL 7.0 SP4 (http://support.microsoft.com/kb/889543) or higher to resolve theses issues.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
889543: MS SQL 7 (http://support.microsoft.com/kb/889543)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2000-1081
Description:	Microsoft SQL Server 7.0/2000 / Data Engine 1.0/2000 - xp_displayparamstmt Buffer Overflow - The Exploit-DB Ref : 20451
Link:	http://www.exploit-db.com/exploits/20451

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

■■■■□ 4 Multiple MS-SQL-7 threats - (II)

QID:	19059
Category:	Database
CVE ID:	CVE-2000-0202, CVE-2002-0643, CVE-2002-0721
Vendor Reference:	-
Bugtraq ID:	5203, 1041
Service Modified:	11/13/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

We can remotely detect the presence of Microsoft's SQL Server, but cannot remotely detect if a patch or service pack has already been applied. Verify that you have applied the appropriate patch and/or service pack.
The following threats are present in MS-SQL-7:
1) Microsoft SQL Server Non-Validated Query Vulnerability. SQL Server 7.0 and Data Engine (SQL-compatible add-on for Access 2000 and Visual Studio 6.0) will accept SQL queries that can lead to a compromise of the database or the underlying operating system. It's possible for any SQL-authenticated user to pass commands through SQL SELECT statements, which will be run at the privilege level of the database owner or administrator.

2) Microsoft SQL Server Installation Password Caching Vulnerability. During the initial installation of Microsoft SQL Server 7 (including MSDE 1.0) or the installation of service packs, information is gathered and stored in a special file that can later be used to automate other MS-SQL Server installations. This file, setup.iss, may contain passwords supplied during the installation process. In addition, the log file documenting the installation process will also contain any passwords entered. The passwords are first encrypted and then stored. The Microsoft released bulletin notes that the encryption may potentially be weak. During the installation process, passwords may be stored in either of the following two cases:

If the SQL Server is being set up in "Mixed Mode", a password for the SQL Server administrator (the ?sa? account) must be supplied.
Whether in Mixed Mode or Windows Authentication Mode, a User ID and password can optionally be supplied for the purpose of starting up SQL Server service accounts.
Contributing to the vulnerability (in versions of SQL Server 7.0), this file is stored on the server in a location that can be viewed by anyone with rights to log on interactively.
3) Microsoft SQL Agent Jobs Privilege Elevation Vulnerability. SQL Server uses an Agent, which is responsible for restarting the SQL Server service, replication, and running scheduled jobs. Some of the jobs supplied by Microsoft as stored procedures on the SQL Server contain weak permissions. The following procedures are affected:
sp_add_job, sp_add_jobstep, sp_add_jobserver, and sp_start_job.
The Agent typically runs in the security context of the SQL Server Service Account. Under normal circumstances, when a T-SQL job is submitted to the Agent, it will drop its privilege level by performing the following command: SETUSER N'guest' WITH NORESET
4) Microsoft SQL Server Extended Stored Procedure Privilege Elevation Vulnerability. Some of the extended stored procedures supplied by Microsoft contain weak permissions. The extended stored procedures typically connect to the database in the security context of the SQL Server Service Account. Users with low privileges could pass certain arguments to the vulnerable extended stored procedures, allowing them to perform actions on the database in the security context of the SQL Server Service Account. The vulnerability could also be exploited by an attacker visiting a Web site that uses one of these extended stored procedures as part of a search engine for the database. The database-driven Web application would need to be prone to existing input validation vulnerabilities for this type of exploitation to occur.
Note: This would appear as a potential for MSSQL versions 8, 9 and above for an unauthenticated scan. MSSQL versions 8,9 and above are not vulnerable for these issues.

IMPACT:

1) The successful exploitation of this vulnerability could lead to a compromise of the database or underlying operating system.
2) If exploited by a malicious user, passwords stored in setup.iss, which are supplied during the installation process, may be stolen.
3) By exploiting this vulnerability, a malicious user would be able to execute other extended stored procedures, such as xp_cmdshell, on the SQL Server with the security context of the SQL Server Service Account.
4) If this vulnerability is exploited, a user with low privileges may perform actions on the database in the security context of the SQL Server Service Account.

SOLUTION:

1) This can be bypassed by causing the Agent to reconnect after it has performed the privilege lowering command. A malicious user can achieve this using the extended stored procedures discussed in the Microsoft SQL Server Extended Stored Procedure Privilege Elevation Vulnerability (BID 5481). It is not currently clear if this issue was addressed in Microsoft Security Bulletin MS02-043 (http://www.microsoft.com/technet/security/bulletin/MS02-043.mspx). However, applying the patch for that issue will significantly mitigate potential exploitation of this vulnerability by preventing attackers from using the vulnerable extended stored procedures to cause the SQL Server Agent to reconnect to the database with a higher privilege level. The bulletin includes instructions for obtaining the patch. Check for upgrades at Microsoft's Download site (http://www.microsoft.com/sql/downloads/default.asp).
2) Microsoft released the following fix for SQL server 7.0: Patch Q327068 (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q327068&sd=tech)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
889543: MS SQL 7 (http://support.microsoft.com/kb/889543)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2002-0721
Description:	Microsoft SQL 2000/7.0 - Agent Jobs Privilege Escalation - The Exploit-DB Ref : 21718
Link:	http://www.exploit-db.com/exploits/21718

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

No results available

Information Gathered (41)

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016/2019/10	NTLMSSP	
Windows Server 2019 Standard 17763/Windows Server 2019 Standard 6.3	CIFS via TCP Port 445	

■■□□□ 2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Message Queuing - QM2QM V1	1.0	2105, 2107, 2103, 49699			
Message Queuing - QMRT V1	1.0	2105, 2107, 2103, 49699			
Message Queuing - QMRT V2	1.0	2105, 2107, 2103, 49699			
Message Queuing - RemoteRead V1	1.0	2105, 2107, 2103, 49699			
Microsoft Local Security Architecture	0.0	49668, 49667			
Microsoft LSA DS Access	0.0	49668, 49667			
Microsoft Network Logon	1.0	49668, 49667			
Microsoft Security Account Manager	1.0	49668, 49667			
(Unknown Service)	1.0	49668, 49667			
(Unknown Service)	0.0	2105, 2107, 2103, 49699			
(Unknown Service)	1.0	2105, 2107, 2103, 49699			
(Unknown Service)	0.0	49668, 49667			
(Unknown Service)	2.0	49668, 49667			
(Unknown Service)	1.0	49664			

■■□□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1
```

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.20.22	qa-db1.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 443, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-134,136-381,383-444,446-1432,1434-1800,1802-2102,2104,2106,2108-2868,
2870-3388,3390-5984,5986-6128,6130-25342,25344-47000,47002-49663,49666,
49669-49687,49689-49692,49694-49698,49701-49710,49712-49724,49726-61192,
61194-65535

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 2453 seconds

Start time: Sat, Feb 20 2021, 06:12:48 GMT

End time: Sat, Feb 20 2021, 06:53:41 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
qa-db1.enterate.com	NTLM DNS
qa-db1.enterate.com	FQDN
qa-db1	NTLM NetBIOS

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547 (https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.
```

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	135	0:07:42
TCP	445	0:01:11
TCP	1433	0:01:28
TCP	3389	0:00:51
TCP	5985	0:27:41
TCP	47001	0:27:42
TCP	49664	0:05:05
TCP	49665	0:05:05
TCP	49667	0:05:05
TCP	49668	0:05:05
TCP	49688	0:05:05
TCP	49693	0:05:05
TCP	49699	0:05:05
TCP	49700	0:05:05
TCP	49711	0:05:05
TCP	49725	0:05:05

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session

Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1433	ms-sql-s	Microsoft-SQL-Server	mssql	
1801	msmq	Microsoft Message Que	Microsoft Message Queue Server	
2103	zephyr-clt	Zephyr serv-hm connection	msrpc	
2105	minipay	MiniPay	msrpc	
2107	unknown	unknown	msrpc	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
47001	unknown	unknown	http	
49664	unknown	unknown	msrpc	
49665	unknown	unknown	msrpc	
49667	unknown	unknown	msrpc	
49668	unknown	unknown	msrpc	
49688	unknown	unknown	msrpc	
49693	unknown	unknown	msrpc	

49699	unknown	unknown	msrpc
49700	unknown	unknown	msrpc
49711	unknown	unknown	msrpc
49725	unknown	unknown	msrpc

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	06:12:48 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The NetBIOS host name of this computer has been detected.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

qa-db1

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1239673680 with a standard deviation of 613919531. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5109 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2
Duration: 20 milli seconds
```

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-db1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:17:41 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-db1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:17:44 GMT
Connection: close
```

```
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
HTTP header and method information collected on port 47001.

GET / HTTP/1.0
Host: qa-db1.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:17:41 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	

(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32

(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb

(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

▮▯▯▯▯ 1 SSL Server Information Retrieval port 1433/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 1433/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance — port 1433/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods — port 1433/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	secp521r1	521	yes	260	low
ECDHE	secp384r1	384	yes	192	low
ECDHE	secp256r1	256	yes	128	low

■□□□□ 1 SSL/TLS Protocol Properties port 1433/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 1433/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information port 1433/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 1433/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 1433/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption

(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:

(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	

countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2

(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-db1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:32:05 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-db1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:32:08 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: qa-db1.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 06:32:05 GMT
Connection: close
Content-Length: 315
```

172.17.20.23 (qa-web2.enterate.com, QA-WEB2) Windows 2012 R2 Standard

Information Gathered (60)

■■■□□ 3 HTTP Public-Key-Pins Security Header Not Detected port 443/tcp

QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/11/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.
QID Detection Logic:

This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.0
Host: qa-web2.enterate.com
```

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2012 R2 Standard	CIFS via TCP Port 445	
Windows 2012 R2/8.1	NTLMSSP	
Windows Vista / Windows 2008	TCP/IP Fingerprint	U3423:80

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
Microsoft Local Security Architecture	0.0	49155, 49156			
Microsoft LSA DS Access	0.0	49155, 49156			
Microsoft Network Logon	1.0	49155, 49156			
Microsoft Scheduler Control Service	1.0	49154			
Microsoft Security Account Manager	1.0	49155, 49156			
Microsoft Server Service	3.0	49154			
Microsoft Task Scheduler	1.0	49154			
MS Wbem Transport IEnumWbemClassObject	0.0	49154			
MS Wbem Transport IWbemLevel1Login	0.0	49154			
MS Wbem Transport IWbemObjectSink	0.0	49154			
MS Wbem Transport IWbemServices	0.0	49154			
(Unknown Service)	1.0	49155, 49156			
(Unknown Service)	0.0	49154			
(Unknown Service)	1.0	49154			

(Unknown Service)	0.0	49155, 49156
(Unknown Service)	4.0	49154
(Unknown Service)	1.0	49152

■■□□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Based on TCP timestamps obtained via port 80, the host's uptime is 8 days, 19 hours, and 51 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.
```

■■□□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

■■□□□ 2 Microsoft ASP.NET HTTP Handlers Enumerated port 443/tcp

QID:	12033
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Microsoft ASP.NET HTTP handlers are used for processing Web requests for specific file extensions. For example, .aspx is used for ASP.NET pages, .rem and .soap are used for remoting, .asmx is used for Web services. These extensions are located in the "machine.config" file under the "httpHandlers" element.
The scanner enummerated the common HTTP handlers present on the target ASP.NET system, and these handlers are displayed in the Results section below.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

■■□□□ 2 Microsoft IIS ISAPI Application Filters Mapped To Home Directory port 443/tcp

QID:	12049
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scanner enumerated the ISAPI filters mapped to the target Microsoft Internet Information Services (IIS) Web server's home directory "/". These are listed in the Result section below.

IMPACT:

Most of the ISAPI filters come by default with IIS, and typically most of them are never used in Web applications. Further, there have been quite a few buffer overflow based remote code execution or denial of service attacks reported for many of these ISAPI filters.

SOLUTION:

Disable the ISAPI filters not being used on the target. This can be done using the "Internet Information Services" MMC snap-in's "Home Directory" section (under "Configuration").
Microsoft provides a free tool named LockDown to secure IIS. LockDown
is available at : http://www.microsoft.com/technet/security/tools/locktool.mspx (http://www.microsoft.com/technet/security/tools/locktool.mspx).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

.Aspx,.Asmx,.Rem,.Soap,

2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1
```

2 Web Server HTTP Protocol Versions port 5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.20.23	qa-web2.enterate.com

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 111, 1, 7, 11.

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-134,136-442,444,446-1705,1707-1999,2001-2146,2148-2512,2514-2701,
2703-2868,2870-3388,3390-5630,5632-5984,5986-6128,6130-11606,11608-42423,
42425-47000,47002-49151,49157-49177,49180-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 2323 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:15:50 GMT

▮▯▯▯▯ 1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
qa-web2.enterate.com	NTLM DNS
qa-web2.enterate.com	FQDN
QA-WEB2	NTLM NetBIOS

■□□□□ 1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:
SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:
Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:
N/A

SOLUTION:
For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:49:19
TCP	135	0:07:35
TCP	443	0:54:35
TCP	445	0:00:02
TCP	3389	0:00:22
TCP	5985	0:36:21
TCP	47001	0:34:06
TCP	49152	0:05:05
TCP	49153	0:05:05
TCP	49154	0:05:08
TCP	49155	0:05:10
TCP	49156	0:05:05
TCP	49178	0:05:05
TCP	49179	0:05:05

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
47001	unknown	unknown	http	
49152	unknown	unknown	msrpc	
49153	unknown	unknown	msrpc	
49154	unknown	unknown	msrpc	
49155	unknown	unknown	msrpc	
49156	unknown	unknown	msrpc	
49178	unknown	unknown	msrpc	
49179	unknown	unknown	msrpc	

■□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:37:11 GMT

1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QA-WEB2

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1171236348 with a standard deviation of 698807212. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5089 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 80: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 23 milli seconds
```

1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web2.enterate.com


<head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a HREF="https://qa-web2.enterate.com/">here</a></body>
```

1 HTTP Response Method and Header Information Collected port 80/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

```
GET / HTTP/1.0
Host: qa-web2.enterate.com



HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: https://qa-web2.enterate.com/
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:38:30 GMT
Connection: keep-alive
Content-Length: 152
```

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected port 80/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubdomains

■□□□□ 1 List of Web Directories port 80/tcp

QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/10/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Directory	Source
/admin/	web page
/help/	web page
/install/	web page
/secure/	web page
/manager/	web page

■□□□□ 1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web2.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:44:59 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}
```

```
-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web2.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:46:50 GMT
Connection: keep-alive
Content-Length: 701

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
 color:#000000;
 background-color:#0072C6;
 margin:0;
}

#container {
 margin-left:auto;
 margin-right:auto;
 text-align:center;
 }

a img {
 border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

▮□□□□ 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE

SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

▮▯▯▯▯ 1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

▮▯▯▯▯ 1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server

OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 443/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good
```

1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:

(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:

(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)

(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

▮▯▯▯▯ 1 HTTP Methods Returned by OPTIONS Request port 443/tcp

QID: 45056

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Allow: OPTIONS, TRACE, GET, HEAD, POST
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 443.

```
GET / HTTP/1.0
Host: qa-web2.enterate.com



HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Sat, 18 Nov 2017 02:20:23 GMT
Accept-Ranges: bytes
ETag: "f73ef6c91360d31:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:44:59 GMT
Connection: keep-alive
Content-Length: 701
```

1 Referrer-Policy HTTP Security Header Not Detected port 443/tcp

QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:
1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin
QID Detection Logic(Unauthenticated):
If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.
References:
- https://www.w3.org/TR/referrer-policy/ (https://www.w3.org/TR/referrer-policy/)
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Referrer-Policy HTTP Header missing on 443 port.

1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubdomains

1 Microsoft IIS ASP.NET Version Obtained port 443/tcp

QID:	86484
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/25/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The ASP.NET version running on the Microsoft IIS Server has been retrieved.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
X-AspNet-Version: 4.0.30319
```

1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:02 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:51:10 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 HTTP Response Method and Header Information Collected port 5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: qa-web2.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:49:02 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web2.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:55:05 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: qa-web2.enterate.com:47001
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:55:11 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

▮□□□□ 1 HTTP Response Method and Header Information Collected port 47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: qa-web2.enterate.com:47001


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:55:05 GMT
Connection: close
Content-Length: 315
```

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

■□□□□ 1 SSL Certificate Transparency Information — port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			
Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT

Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a0942875e4e318b1b03ebeb4bc768f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

■□□□□ 1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

■□□□□ 1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	

(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)
(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32

(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb

(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.30.15 (util17-1.enterate.com, UTIL17-1) Windows 2016

Vulnerabilities (1)

■□□□□ 1 SSL/TLS Server supports TLSv1.1 port 3391/udp over SSL

QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/22/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.
This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

IMPACT:

Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:

Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:

```
openssl s_client -connect ip:port -tls1_1
```

If the test is successful, then the target support TLSv1.1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.1 is supported

Information Gathered (65)

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Windows 2016	CIFS via TCP Port 445	
Windows 2016/2019/10	NTLMSSP	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:80
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	

2 Open DCE-RPC / MS-RPC Services List

QID:	70022
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/22/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:
N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0			593	
DCOM OXID Resolver	0.0			593	
DCOM Remote Activation	0.0			593	
DCOM System Activator	0.0	64088		593	
Microsoft Local Security Architecture	0.0	49667, 49686			
Microsoft LSA DS Access	0.0	49667, 49686			
Microsoft Network Logon	1.0	49667, 49686			
Microsoft Scheduler Control Service	1.0	64088			\PIPE\atsvc
Microsoft Security Account Manager	1.0	49667, 49686			\pipe\lsass

Microsoft Service Control Service	2.0	64093		
Microsoft Task Scheduler	1.0	64088		\PIPE\atsvc
MS Wbem Transport IEnumWbemClassObject	0.0	64088		
MS Wbem Transport IWbemLevel1Login	0.0	64088		
MS Wbem Transport IWbemObjectSink	0.0	64088		
MS Wbem Transport IWbemServices	0.0	64088		
MSIE IRegExp2	0.0	64088		
WinHttp Auto-Proxy Service	5.1			\PIPE\W32TIME_ALT
(Unknown Service)	1.0		593	
(Unknown Service)	1.0	49667, 49686		
(Unknown Service)	0.0	64088	3388	
(Unknown Service)	0.0	64088		
(Unknown Service)	0.0		593	
(Unknown Service)	1.0	64088		
(Unknown Service)	2.0		593	
DCOM Class Factory	0.0	64088		
(Unknown Service)	0.0	49667, 49686		
(Unknown Service)	0.0	49667, 49686		\pipe\lsass
(Unknown Service)	2.0	49667, 49686		\pipe\lsass
(Unknown Service)	1.0	49667, 49686		\pipe\lsass
(Unknown Service)	1.0	49664		
(Unknown Service)	1.0	49664		\PIPE\InitShutdown
(Unknown Service)	1.3		3388	
(Unknown Service)	1.0		3388	
(Unknown Service)	4.0	64088		
(Unknown Service)	2.0	64088		\PIPE\atsvc
(Unknown Service)	1.0	64088		\PIPE\atsvc
(Unknown Service)	1.0	64088		\pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0	64088, 49665		\pipe\LSM_API_service, \pipe\eventlog, \pipe\SessEnvPublicRpc, \PIPE\atsvc
(Unknown Service)	1.0			\pipe\LSM_API_service
(Unknown Service)	0.0			\pipe\LSM_API_service
(Unknown Service)	1.0	49665		\pipe\eventlog
Event log TCPIP	1.0	49665		\pipe\eventlog
DHCPv6 Client LRPC Endpoint	1.0			\pipe\eventlog
DHCP Client LRPC Endpoint	1.0			\pipe\eventlog
DfsDs service	1.0			\PIPE\wkssvc
Remote Fw APIs	1.0	64087		
(Unknown Service)	1.0	64120		

■■□□□ 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Based on TCP timestamps obtained via port 80, the host's uptime is 4 days, 14 hours, and 12 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

■■□□□ 2 Windows Registry Pipe Access Level

QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:

Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:

Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Access to Remote Registry Service is denied, error: 0x0

■■□□□ 2 Web Server HTTP Protocol Versions rdg.enterate.com:80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1
```

■■□□□ 2 Web Server HTTP Protocol Versions rdg.enterate.com:443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions rdg.enterate.com:47001/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 47001 port.GET / HTTP/1.1

■■□□□ 2 Web Server HTTP Protocol Versions rdg.enterate.com:5985/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Remote Web Server supports HTTP version 1.x on 5985 port.GET / HTTP/1.1

■□□□□ 1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.30.15	rdg.enterate.com

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-79,81-134,136-442,444,446-592,594-1705,1707-1915,1917-1999,2001-2146,
2148-2512,2514-2701,2703-2868,2870-3387,3390-5630,5632-5984,5986-6128,
6130-42423,42425-47000,47002-49663,49666,49668-49685,49687-64086,64089-64092,
64094-64119,64121-65535
```

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2329 seconds

Start time: Sat, Feb 20 2021, 05:36:39 GMT

End time: Sat, Feb 20 2021, 06:15:28 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/26/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
util17-1.enterate.com	NTLM DNS
rdg.enterate.com	FQDN
UTIL17-1	NTLM NetBIOS

1 SMB Version 1 Enabled

QID:	45261
Category:	Information gathering
CVE ID:	-
Vendor Reference:	SMB v1
Bugtraq ID:	-
Service Modified:	09/18/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol.
The Windows host has SMBv1 protocol enabled for either :
Client or
Server

IMPACT:

SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

SOLUTION:

Microsoft recommends users to update to latest SMB versions and stop using SMBv1.
Refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012)
for more details.

Workaround:Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445
with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 45261 detected on port 445 over TCP.
SMBv1 is enabled.

▮▯▯▯▯ 1 SMB Version 2 or 3 Enabled

QID:	45262
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/29/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Windows host has SMBv2 or SMBv3 protocol enabled.

IMPACT:

N/A

SOLUTION:

For more information on how to enable/disable SMB, refer to Microsoft KB article KB2696547
(https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
QID: 45262 detected on port 445 over TCP.
SMBv2 is enabled.

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	80	0:41:18
TCP	135	0:08:06
TCP	443	0:49:28
TCP	445	0:00:01
TCP	593	0:00:45
TCP	3388	0:00:45
TCP	3389	0:00:51
TCP	5985	0:35:19
TCP	47001	0:34:42
TCP	49664	0:05:05
TCP	49665	0:05:05
TCP	49667	0:05:05
TCP	49686	0:05:05

TCP	64087	0:05:05
TCP	64088	0:05:05
TCP	64093	0:05:05
TCP	64120	0:05:05
UDP	3391	0:01:37

1 Microsoft Server Message Block (SMBv3) Compression Disabled

QID:	48086
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/13/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The remote host supports Microsoft Server Message Block 3.1.1 (SMBv3) protocol with compression feature disabled.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Microsoft Server Message Block (SMBv3) Compression Disabled

1 Windows Authentication Method

QID:	70028
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/09/2008
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Disabled
Discovery Method	NULL session, no valid login credentials provided or found
CIFS Signing	default

■□□□□ 1 File and Print Services Access Denied

QID:	70038
Category:	SMB / NETBIOS
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Remote Access to File and Print Services did not succeed. This is provided by Common Internet File System (CIFS) service. If you provided Windows
Authentication credentials, the Windows Authentication Method QID or the Windows Authentication Failed QID will not be reported if this service is not running.

IMPACT:
Vulnerabilities that require authenticated access may not be reported.

SOLUTION:
On a Windows host, make sure that the network setting for File and Print Services is enabled and the "Server" service (CIFS) is running.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

■□□□□ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
3391	savant	SAVANT	DTLS

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
80	www-http	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	unknown	
443	https	http protocol over TLS/SSL	http over ssl	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
593	http-rpc-epmap	HTTP RPC Ep Map	msrpc-over-http	
3388	cbserver	CB Server	msrpc-over-http	
3389	ms-wbt-server	MS WBT Server	CredSSP over ssl	
5985	unknown	unknown	http	
47001	unknown	unknown	http	
49664	unknown	unknown	msrpc	
49665	unknown	unknown	msrpc	
49667	unknown	unknown	msrpc	
49686	unknown	unknown	msrpc	
64087	unknown	unknown	msrpc	
64088	unknown	unknown	msrpc	
64093	unknown	unknown	msrpc	
64120	unknown	unknown	msrpc	

▮□□□□ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	05:36:40 GMT

▮▯▯▯▯ 1 NetBIOS Host Name

QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/20/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

UTIL17-1

▮▯▯▯▯ 1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 911932016 with a standard deviation of 550095385. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5101 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 80: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 19 milli seconds

1 Default Web Page port 80/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:37:51 GMT
Connection: keep-alive
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
```

```
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 80/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:38:07 GMT
Connection: keep-alive
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
```

```
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 80/tcp

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.30.15:80

GET /Q_Evasive/ HTTP/1.1
Host:172.17.30.15:80
```

```
HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 06:13:27 GMT
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>
HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 06:13:27 GMT
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
```

```
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

▮▯▯▯▯ 1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:41:09 GMT
Connection: keep-alive
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
```

```
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 443/tcp over SSL

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:

N/A

SOLUTION:

N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:42:23 GMT
Connection: keep-alive
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

▮□□□□ 1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

■□□□□ 1 SSL Session Caching Information port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

■□□□□ 1 SSL/TLS Key Exchange Methods port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

1 SSL Certificate OCSP Information port 443/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=rdg.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 443/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=rdg.enterate.com, OU=Domain Control Validated			
Certificate	yes	Google 'Pilot' log	ct.googleapis.com/pilot/	a4b90990b418581487bb13a2cc67700a3c359804f91bdfb8e377cd0ec80ddc10	Mon 18 May 2020 11:15:29 AM GMT
Certificate	yes	Google 'Skydiver' log	ct.googleapis.com/skydiver/	bbd9dfbc1f8a71b593942397aa927b473857950aab52e81a909664368e1ed185	Mon 18 May 2020 11:15:29 AM GMT
Certificate	yes	DigiCert Log Server	ct1.digicert-ct.com/log/	5614069a2fd7c2ecd3f5e1bd44b23ec74676b9bc99115cc0ef949855d689d0dd	Mon 18 May 2020 11:15:30 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as

the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 443/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	35:3b:be:81:b7:f5:43:0c
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona

localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	rdg.enterate.com
(0)Valid From	May 18 11:15:28 2020 GMT
(0)Valid Till	Jul 18 01:15:33 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c7:94:fc:c9:c6:0f:67:a7:16:7d:f2:e2:90:10:
(0)	48:95:98:6c:81:bf:9b:ac:50:cb:e4:08:2d:65:74:
(0)	88:ae:a2:66:f2:5e:c4:04:10:23:4b:ff:c0:aa:d1:
(0)	6b:38:8e:bd:c7:d0:2f:f2:4d:11:0d:99:d4:48:95:
(0)	fe:c0:9a:9e:99:ff:76:32:e4:2f:c3:45:f0:a4:b5:
(0)	e7:1d:f6:cb:a0:af:67:03:4c:6a:bd:aa:22:f1:d1:
(0)	b7:d5:8f:9d:1d:43:62:2d:dc:f3:7d:38:51:b0:b3:
(0)	ea:d8:b8:9a:cd:dc:dc:54:cf:8c:01:e7:38:4b:d1:
(0)	b1:16:ee:16:84:0d:89:7d:64:ba:b0:77:a8:dc:8c:
(0)	88:99:5a:e6:79:bd:a7:fa:bf:9e:4b:27:37:2b:45:
(0)	3b:4d:28:30:c6:a8:83:b3:58:bc:a3:fd:64:02:00:
(0)	3c:10:11:48:e8:af:25:96:43:6b:dd:17:10:dd:73:
(0)	a5:0d:11:d8:58:1a:17:00:cb:13:b7:ab:15:97:7e:
(0)	90:97:eb:38:88:53:aa:f6:c0:85:1e:6c:be:64:74:
(0)	48:ba:78:fe:e2:10:02:19:e6:f4:98:a8:0d:ce:38:
(0)	17:0a:df:53:f7:ad:46:30:78:9a:b2:ab:52:70:e0:
(0)	d8:a6:e6:a1:ed:ad:0c:08:6d:ac:07:71:68:dc:e0:
(0)	6c:f9
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-1972.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:rdg.enterate.com, DNS:www.rdg.enterate.com, DNS:qa-web1.enterate.com, DNS:web1.enterate.com
(0)X509v3 Subject Key Identifier	70:D4:47:52:36:50:C5:11:9B:F6:72:3C:ED:34:62:36:DE:FF:85:AB
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
(0)	3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
(0)	Timestamp : May 18 11:15:29.271 2020 GMT

(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:D4:2B:E7:DE:66:C3:9E:F5:AF:71:65:
(0)	6F:C0:3D:C3:C3:A4:40:64:E1:9F:8D:61:7D:8B:33:DE:
(0)	58:54:B8:59:54:02:21:00:BB:46:24:BD:59:18:AF:62:
(0)	AA:EC:27:90:34:B5:26:19:0B:45:EF:38:29:88:CF:08:
(0)	27:1D:B8:E4:63:FD:03:15
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : BB:D9:DF:BC:1F:8A:71:B5:93:94:23:97:AA:92:7B:47:
(0)	38:57:95:0A:AB:52:E8:1A:90:96:64:36:8E:1E:D1:85
(0)	Timestamp : May 18 11:15:29.932 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:20:56:EC:A4:48:42:65:69:57:19:92:58:90:
(0)	E4:A2:35:77:3B:EF:92:E0:EB:8F:D4:9F:BF:49:BF:01:
(0)	C9:99:71:73:02:20:6C:6D:E2:9E:B3:AA:B2:EF:28:35:
(0)	2F:B4:CC:D6:96:8A:9C:DC:41:49:11:5E:13:04:7C:24:
(0)	22:55:8B:AF:3C:E3
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 56:14:06:9A:2F:D7:C2:EC:D3:F5:E1:BD:44:B2:3E:C7:
(0)	46:76:B9:BC:99:11:5C:C0:EF:94:98:55:D6:89:D0:DD
(0)	Timestamp : May 18 11:15:30.513 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:3C:A4:5A:84:5C:22:63:B2:4B:80:08:58:
(0)	39:09:CA:BD:21:6E:B6:82:B1:02:59:81:C0:41:2B:50:
(0)	B6:DB:FF:66:02:21:00:DB:50:07:D7:EE:31:2F:FF:EE:
(0)	8B:25:93:55:1B:34:69:52:85:A2:6A:54:3D:3D:3C:26:
(0)	30:5D:C8:41:30:18:B6
(0)Signature	(256 octets)
(0)	66:0e:56:73:ed:ab:74:cd:ae:a5:85:ba:9b:f0:18:89
(0)	15:8f:65:4a:05:c6:79:e0:03:28:d8:81:64:af:ef:8d
(0)	ca:35:48:b6:b7:d8:61:1e:bd:af:5a:34:ff:bb:41:e5
(0)	ff:4f:4e:09:c5:d9:a5:8d:4e:29:74:31:f8:a3:f4:d1
(0)	b9:de:96:82:57:77:bc:00:0b:5f:7c:61:8a:30:78:fd
(0)	00:f2:91:73:83:4e:cb:9e:9a:93:26:3d:97:09:9c:16
(0)	e1:e8:19:95:46:a2:8f:26:e5:56:b8:07:37:1d:74:ec
(0)	d3:16:2b:58:f4:07:3a:70:c5:e4:f6:0f:da:59:36:bd
(0)	61:04:c0:85:17:c8:5e:40:aa:e3:54:87:83:ea:6c:dc
(0)	42:fa:41:e9:5b:fc:04:5e:da:fc:1a:8d:28:72:c7:32
(0)	c2:f1:3a:ca:6b:a2:23:04:45:e6:4f:37:e9:7e:c6:4d
(0)	75:e8:e9:ba:7c:34:a7:7b:27:5e:89:c7:7c:7c:15:f1
(0)	2a:2f:5f:51:25:8a:9b:c6:e7:ab:45:4f:11:7f:cd:90
(0)	91:1a:2a:d8:06:35:f5:82:75:63:ad:c2:c4:16:88:b5
(0)	97:c2:f7:b7:eb:75:83:31:02:c2:ad:2d:c3:82:5d:3e
(0)	4c:6b:6c:2a:86:aa:8f:56:3e:8c:d5:c8:34:f1:51:f3
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona

localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8

(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

■□□□□ 1 Web Server Supports HTTP Request Pipelining port 443/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:

Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:172.17.30.15:443

GET /Q_Evasive/ HTTP/1.1
Host:172.17.30.15:443



HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
```

```
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 06:13:27 GMT
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>
HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 06:13:27 GMT
Content-Length: 1208

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

1 HTTP Response Method and Header Information Collected rdg.enterate.com:80/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 80.

```
GET / HTTP/1.0
Host: rdg.enterate.com


HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:37:51 GMT
Connection: keep-alive
Content-Length: 1208
```

1 HTTP Strict Transport Security (HSTS) Support Detected rdg.enterate.com:80/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Strict-Transport-Security: max-age=31536000; includeSubdomains
```

■□□□□ 1 HTTP Response Method and Header Information Collected rdg.enterate.com:443/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 443.

```
GET / HTTP/1.0
Host: rdg.enterate.com



HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Content-Security-Policy: default-src https: data: 'unsafe-inline' 'unsafe-eval'
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubdomains
Date: Sat, 20 Feb 2021 05:41:09 GMT
Connection: keep-alive
Content-Length: 1208
```

■□□□□ 1 HTTP Strict Transport Security (HSTS) Support Detected rdg.enterate.com:443/tcp

QID:	86137
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubdomains

■□□□□ 1 Default Web Page port 47001/tcp

QID:	12230
Category:	CGI

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com:47001


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:44:52 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

■□□□□ 1 Default Web Page (Follow HTTP Redirection) port 47001/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com:47001



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:46:45 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected rdg.enterate.com:47001/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP header and method information collected on port 47001.

```
GET / HTTP/1.0
Host: rdg.enterate.com:47001


HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:44:52 GMT
Connection: close
Content-Length: 315
```

■□□□□ 1 SSL Server Information Retrieval port 3391/udp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
DTLSv1 PROTOCOL IS ENABLED					
DTLSv1	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH

ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
DTLSv1.2 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3391/udp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

DTLSv1 session caching is disabled on the target.

1 SSL/TLS Key Exchange Methods port 3391/udp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
DTLSv1					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

■□□□□ 1 SSL/TLS Protocol Properties port 3391/udp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
DTLSv1	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	no
SCT extension	no

■□□□□ 1 SSL Certificate Transparency Information port 3391/udp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=rdg.enterate.com, OU=Domain Control Validated			
Certificate	yes	Google 'Pilot' log	ct.googleapis.com/pilot/	a4b90990b418581487bb13a2cc67700a3c359804f91bdfb8e377cd0ec80ddc10	Mon 18 May 2020 11:15:29 AM GMT
Certificate	yes	Google 'Skydiver' log	ct.googleapis.com/skydiver/	bbd9dfbc1f8a71b593942397aa927b473857950aab52e81a909664368e1ed185	Mon 18 May 2020 11:15:29 AM GMT
Certificate	yes	DigiCert Log Server	ct1.digicert-ct.com/log/	5614069a2fd7c2ecd3f5e1bd44b23ec74676b9bc99115cc0ef949855d689d0dd	Mon 18 May 2020 11:15:30 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3391/udp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3391/udp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL certificate information is provided in the Results section.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	35:3b:be:81:b7:f5:43:0c
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	rdg.enterate.com
(0)Valid From	May 18 11:15:28 2020 GMT
(0)Valid Till	Jul 18 01:15:33 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:c7:94:fc:c9:c6:0f:67:a7:16:7d:f2:e2:90:10:
(0)	48:95:98:6c:81:bf:9b:ac:50:cb:e4:08:2d:65:74:
(0)	88:ae:a2:66:f2:5e:c4:04:10:23:4b:ff:c0:aa:d1:
(0)	6b:38:8e:bd:c7:d0:2f:f2:4d:11:0d:99:d4:48:95:
(0)	fe:c0:9a:9e:99:ff:76:32:e4:2f:c3:45:f0:a4:b5:
(0)	e7:1d:f6:cb:a0:af:67:03:4c:6a:bd:aa:22:f1:d1:
(0)	b7:d5:8f:9d:1d:43:62:2d:dc:f3:7d:38:51:b0:b3:
(0)	ea:d8:b8:9a:cd:dc:dc:54:cf:8c:01:e7:38:4b:d1:
(0)	b1:16:ee:16:84:0d:89:7d:64:ba:b0:77:a8:dc:8c:
(0)	88:99:5a:e6:79:bd:a7:fa:bf:9e:4b:27:37:2b:45:
(0)	3b:4d:28:30:c6:a8:83:b3:58:bc:a3:fd:64:02:00:
(0)	3c:10:11:48:e8:af:25:96:43:6b:dd:17:10:dd:73:
(0)	a5:0d:11:d8:58:1a:17:00:cb:13:b7:ab:15:97:7e:
(0)	90:97:eb:38:88:53:aa:f6:c0:85:1e:6c:be:64:74:
(0)	48:ba:78:fe:e2:10:02:19:e6:f4:98:a8:0d:ce:38:
(0)	17:0a:df:53:f7:ad:46:30:78:9a:b2:ab:52:70:e0:
(0)	d8:a6:e6:a1:ed:ad:0c:08:6d:ac:07:71:68:dc:e0:
(0)	6c:f9
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	

(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-1972.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:rdg.enterate.com, DNS:www.rdg.enterate.com, DNS:qa-web1.enterate.com, DNS:web1.enterate.com
(0)X509v3 Subject Key Identifier	70:D4:47:52:36:50:C5:11:9B:F6:72:3C:ED:34:62:36:DE:FF:85:AB
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
(0)	3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
(0)	Timestamp : May 18 11:15:29.271 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:D4:2B:E7:DE:66:C3:9E:F5:AF:71:65:
(0)	6F:C0:3D:C3:C3:A4:40:64:E1:9F:8D:61:7D:8B:33:DE:
(0)	58:54:B8:59:54:02:21:00:BB:46:24:BD:59:18:AF:62:
(0)	AA:EC:27:90:34:B5:26:19:0B:45:EF:38:29:88:CF:08:
(0)	27:1D:B8:E4:63:FD:03:15
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : BB:D9:DF:BC:1F:8A:71:B5:93:94:23:97:AA:92:7B:47:
(0)	38:57:95:0A:AB:52:E8:1A:90:96:64:36:8E:1E:D1:85
(0)	Timestamp : May 18 11:15:29.932 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:20:56:EC:A4:48:42:65:69:57:19:92:58:90:
(0)	E4:A2:35:77:3B:EF:92:E0:EB:8F:D4:9F:BF:49:BF:01:
(0)	C9:99:71:73:02:20:6C:6D:E2:9E:B3:AA:B2:EF:28:35:
(0)	2F:B4:CC:D6:96:8A:9C:DC:41:49:11:5E:13:04:7C:24:
(0)	22:55:8B:AF:3C:E3
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 56:14:06:9A:2F:D7:C2:EC:D3:F5:E1:BD:44:B2:3E:C7:
(0)	46:76:B9:BC:99:11:5C:C0:EF:94:98:55:D6:89:D0:DD
(0)	Timestamp : May 18 11:15:30.513 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:3C:A4:5A:84:5C:22:63:B2:4B:80:08:58:
(0)	39:09:CA:BD:21:6E:B6:82:B1:02:59:81:C0:41:2B:50:
(0)	B6:DB:FF:66:02:21:00:DB:50:07:D7:EE:31:2F:FF:EE:
(0)	8B:25:93:55:1B:34:69:52:85:A2:6A:54:3D:3D:3C:26:
(0)	30:5D:C8:41:30:18:B6
(0)Signature	(256 octets)
(0)	66:0e:56:73:ed:ab:74:cd:ae:a5:85:ba:9b:f0:18:89
(0)	15:8f:65:4a:05:c6:79:e0:03:28:d8:81:64:af:ef:8d
(0)	ca:35:48:b6:b7:d8:61:1e:bd:af:5a:34:ff:bb:41:e5
(0)	ff:4f:4e:09:c5:d9:a5:8d:4e:29:74:31:f8:a3:f4:d1
(0)	b9:de:96:82:57:77:bc:00:0b:5f:7c:61:8a:30:78:fd
(0)	00:f2:91:73:83:4e:cb:9e:9a:93:26:3d:97:09:9c:16
(0)	e1:e8:19:95:46:a2:8f:26:e5:56:b8:07:37:1d:74:ec

(0)	d3:16:2b:58:f4:07:3a:70:c5:e4:f6:0f:da:59:36:bd
(0)	61:04:c0:85:17:c8:5e:40:aa:e3:54:87:83:ea:6c:dc
(0)	42:fa:41:e9:5b:fc:04:5e:da:fc:1a:8d:28:72:c7:32
(0)	c2:f1:3a:ca:6b:a2:23:04:45:e6:4f:37:e9:7e:c6:4d
(0)	75:e8:e9:ba:7c:34:a7:7b:27:5e:89:c7:7c:7c:15:f1
(0)	2a:2f:5f:51:25:8a:9b:c6:e7:ab:45:4f:11:7f:cd:90
(0)	91:1a:2a:d8:06:35:f5:82:75:63:ad:c2:c4:16:88:b5
(0)	97:c2:f7:b7:eb:75:83:31:02:c2:ad:2d:c3:82:5d:3e
(0)	4c:6b:6c:2a:86:aa:8f:56:3e:8c:d5:c8:34:f1:51:f3
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:
(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical

(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

▮▯▯▯▯ 1 Default Web Page port 5985/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/15/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:06 GMT
Connection: close
Content-Length: 315

    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 Default Web Page (Follow HTTP Redirection) port 5985/tcp

QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/05/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A
Patch:
Following are links for downloading patches to fix the vulnerabilities:
nas-201911-01 (https://www.qnap.com/en/security-advisory/nas-201911-01)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.0
Host: rdg.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:10 GMT
Connection: close
```

```
Content-Length: 315

      <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

1 HTTP Response Method and Header Information Collected rdg.enterate.com:5985/tcp

QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/20/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.
QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

HTTP header and method information collected on port 5985.

```
GET / HTTP/1.0
Host: rdg.enterate.com:5985



HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 20 Feb 2021 05:56:06 GMT
Connection: close
Content-Length: 315
```

1 SSL Server Information Retrieval port 3389/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS DISABLED					
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH
TLSv1.3 PROTOCOL IS DISABLED					

1 SSL Session Caching Information port 3389/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.2 session caching is enabled on the target.

■□□□□ 1 SSL/TLS invalid protocol version tolerance port 3389/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL/TLS Key Exchange Methods port 3389/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1.2					
RSA		2048	no	110	low
ECDHE	x25519	256	yes	128	low
ECDHE	secp256r1	256	yes	128	low
ECDHE	secp384r1	384	yes	192	low

1 SSL/TLS Protocol Properties port 3389/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS
TLSv1.2	
Extended Master Secret	yes
Encrypt Then MAC	no
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	server
OCSP stapling	yes
SCT extension	no

■□□□□ 1 SSL Certificate OCSP Information port 3389/tcp over SSL

QID:	38717
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Certificate #0 CN=*.enterate.com,OU=Domain_Control_Validated OCSP status: good

1 SSL Certificate Transparency Information port 3389/tcp over SSL

QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/22/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".
The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Source	Validated	Name	URL	ID	Time
Certificate #0		CN=*.enterate.com, OU=Domain Control Validated			

Certificate	no	(unknown)	(unknown)	2979bef09e393921f056739f63 a577e5be577d9c600af8f94d5d 265c255dc784	Thu 01 Jan 1970 12:00:00 AM GMT
Certificate	yes	DigiCert Yeti2022 Log	yeti2022.ct.digicert.com/log/	2245450759552456963fa12ff1 f76d86e0232663adc04b7f5dc6 835c6ee20f02	Thu 18 Jun 2020 10:58:25 AM GMT
Certificate	no	(unknown)	(unknown)	41c8cab1df22464a10c6a13a09 42875e4e318b1b03ebeb4bc768 f090629606f6	Thu 01 Jan 1970 12:00:00 AM GMT

1 TLS Secure Renegotiation Extension Support Information port 3389/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

1 SSL Certificate - Information port 3389/tcp over SSL

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	f8:cd:34:7e:b1:62:1e:b3
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(0)SUBJECT NAME	
organizationalUnitName	Domain Control Validated
commonName	*.enterate.com
(0)Valid From	Jun 18 10:58:23 2020 GMT
(0)Valid Till	Aug 17 17:30:12 2022 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	RSA Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:bd:49:0c:65:2f:e6:5c:91:14:7b:93:1d:28:76:
(0)	78:45:70:ae:91:10:b6:d0:ba:b1:60:14:f9:3c:2e:
(0)	47:8e:07:f3:8f:0b:4e:6d:ed:18:be:77:ed:99:55:
(0)	94:e9:eb:50:0f:48:d4:6e:d2:de:da:d6:3d:24:72:
(0)	97:f6:d1:c7:d5:7f:28:69:b9:b0:69:e1:36:14:5d:
(0)	d8:da:c4:b2:63:a0:fa:59:90:6d:bf:99:b0:fb:7a:
(0)	9e:78:03:75:68:15:19:06:ef:ae:29:dc:4f:e9:ce:
(0)	9e:41:c5:58:75:98:49:8d:65:b0:2c:e7:56:c8:84:
(0)	64:19:e9:31:c1:d5:b7:cb:7d:4e:7b:49:d1:ed:ab:
(0)	ad:93:0c:ab:3a:3c:a5:22:4f:70:71:0f:81:37:6a:
(0)	98:38:1b:e4:d5:d2:91:c8:ba:30:97:07:68:2b:d8:
(0)	f5:bf:24:4c:1d:37:7d:6a:b6:29:15:e2:ea:d1:af:
(0)	8c:e8:72:f1:8a:a7:7b:55:90:e4:70:c5:ff:84:fd:
(0)	2b:15:14:d7:47:94:b4:73:99:53:fa:cb:0e:ff:4e:
(0)	e6:b1:60:c0:4a:18:ac:ad:02:7b:b4:8f:27:1e:62:
(0)	df:69:7f:98:4f:0a:13:05:71:59:41:9d:54:57:5a:
(0)	c4:31:86:ce:05:3c:8a:f9:72:67:56:26:47:00:ab:
(0)	6d:95

(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 CRL Distribution Points	
(0)	Full Name:
(0)	URI:http://crl.godaddy.com/gdig2s1-2039.crl
(0)X509v3 Certificate Policies	Policy: 2.16.840.1.114413.1.7.23.1
(0)	CPS: http://certificates.godaddy.com/repository/
(0)	Policy: 2.23.140.1.2.1
(0)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(0)	CA Issuers - URI:http://certificates.godaddy.com/repository/gdig2.crt
(0)X509v3 Authority Key Identifier	keyid:40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(0)X509v3 Subject Alternative Name	DNS:*.enterate.com, DNS:enterate.com
(0)X509v3 Subject Key Identifier	8A:77:88:AF:EC:1F:15:C1:C3:2B:CB:51:0D:08:38:87:D1:41:77:0F
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 29:79:BE:F0:9E:39:39:21:F0:56:73:9F:63:A5:77:E5:
(0)	BE:57:7D:9C:60:0A:F8:F9:4D:5D:26:5C:25:5D:C7:84
(0)	Timestamp : Jun 18 10:58:25.486 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:45:02:20:64:13:46:58:87:D4:EC:A7:4D:DD:74:BA:
(0)	37:B5:80:FD:51:D9:6C:58:90:AF:00:8D:84:83:C8:4B:
(0)	89:2B:E9:64:02:21:00:EA:0B:C2:D0:39:A8:F3:16:E3:
(0)	8C:1B:47:61:24:A8:17:1C:80:73:90:6C:5F:7B:F8:57:
(0)	74:52:59:D9:98:C9:23
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 22:45:45:07:59:55:24:56:96:3F:A1:2F:F1:F7:6D:86:
(0)	E0:23:26:63:AD:C0:4B:7F:5D:C6:83:5C:6E:E2:0F:02
(0)	Timestamp : Jun 18 10:58:25.998 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:CB:61:8B:9C:68:07:9E:0D:A4:92:D2:
(0)	F5:6F:22:72:5E:6E:AC:12:F1:C7:5B:0E:DB:64:42:02:
(0)	51:DE:DB:E3:C7:02:21:00:B7:F0:D3:6E:6E:F6:B5:0B:
(0)	92:B7:C8:65:AE:90:85:7A:C2:6C:12:28:DF:68:F6:35:
(0)	DD:6F:AC:58:43:10:84:53
(0)	Signed Certificate Timestamp:
(0)	Version : v1 (0x0)
(0)	Log ID : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
(0)	4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
(0)	Timestamp : Jun 18 10:58:26.587 2020 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:21:00:DC:B2:08:F2:79:CA:5A:CB:10:D2:B3:
(0)	26:C3:81:35:83:F8:B0:4C:77:8D:E7:D8:85:F2:82:B2:
(0)	FF:28:92:EA:5E:02:1F:32:5C:DB:31:87:53:A1:36:F8:
(0)	29:27:F2:5F:88:94:E8:13:E0:96:EA:E4:9C:6E:0B:96:
(0)	8B:0F:C3:9D:53:A5
(0)Signature	(256 octets)

(0)	3d:7a:f9:d8:f0:08:dd:89:84:c9:68:a6:a5:a5:39:7b
(0)	c3:44:3a:d5:18:ba:63:32:7d:ad:4a:d8:d7:2d:73:32
(0)	9e:f1:c5:7e:48:d5:be:bb:69:b1:7f:f3:41:4a:24:66
(0)	6a:c4:bc:0a:35:a8:d8:9f:7c:64:19:c1:66:f4:37:fe
(0)	c3:d7:2e:ea:2c:7e:52:66:f6:77:38:72:41:0e:a4:9c
(0)	b1:66:e3:a8:fc:82:7b:b3:97:0c:52:c5:6b:28:78:81
(0)	25:9e:b9:25:13:2a:a1:af:f5:d5:a3:73:47:be:3f:6d
(0)	d5:51:a5:d9:db:0b:61:30:aa:a3:9a:8f:4e:4e:7a:21
(0)	d6:16:df:bd:c8:54:8f:3f:63:a7:f9:15:aa:c1:14:00
(0)	ec:e6:65:fc:d0:7a:ea:53:a2:02:43:3b:94:d7:f9:dc
(0)	9b:f6:40:ac:2a:1a:0b:53:ba:c5:5f:d0:19:82:3e:c2
(0)	62:ea:b9:59:9b:47:e7:af:0e:3f:ad:30:ea:62:fd:36
(0)	8c:74:d3:2b:ec:ef:b5:bc:3b:62:ed:bf:ae:b3:50:13
(0)	15:eb:00:76:72:aa:02:e1:33:45:92:8c:1b:1c:c7:4c
(0)	f3:9e:b7:9d:7b:7c:23:0b:65:b5:2b:b9:2f:57:bd:2d
(0)	4c:78:70:f0:37:2d:77:e4:b8:0f:66:2c:74:90:d9:77
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	7 (0x7)
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
commonName	Go Daddy Root Certificate Authority - G2
(1)SUBJECT NAME	
countryName	US
stateOrProvinceName	Arizona
localityName	Scottsdale
organizationName	"GoDaddy.com, Inc."
organizationalUnitName	http://certs.godaddy.com/repository/
commonName	Go Daddy Secure Certificate Authority - G2
(1)Valid From	May 3 07:00:00 2011 GMT
(1)Valid Till	May 3 07:00:00 2031 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	RSA Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64:
(1)	b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf:
(1)	8f:ce:62:e6:3c:52:1c:da:16:45:4b:55:ab:78:6b:
(1)	63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc:
(1)	45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57:
(1)	c4:cf:2e:f4:3f:30:3c:5d:47:fc:9a:16:bc:c3:37:
(1)	96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30:
(1)	38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f:
(1)	38:47:53:d1:46:1d:b4:e3:dc:00:ea:45:ac:bd:bc:
(1)	71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47:
(1)	f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4:
(1)	33:4e:ea:b3:d6:27:4f:ad:25:8a:a5:c6:f4:d5:d0:
(1)	a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e:
(1)	f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a:
(1)	ae:e7:79:33:af:0c:20:07:7f:e8:df:04:39:c2:69:
(1)	02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18:

(1)	50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2:
(1)	52:fb
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE
(1)X509v3 Key Usage	critical
(1)	Certificate Sign, CRL Sign
(1)X509v3 Subject Key Identifier	40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE
(1)X509v3 Authority Key Identifier	keyid:3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE
(1)Authority Information Access	OCSP - URI:http://ocsp.godaddy.com/
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.godaddy.com/gdroot-g2.crl
(1)X509v3 Certificate Policies	Policy: X509v3 Any Policy
(1)	CPS: https://certs.godaddy.com/repository/
(1)Signature	(256 octets)
(1)	08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f
(1)	04:ef:6c:3e:9c:88:06:c9:50:8f:a6:73:f7:57:31:1b
(1)	be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e
(1)	0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2
(1)	5d:90:d7:b4:7c:25:4f:11:56:30:c4:b6:44:9d:7b:2c
(1)	9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8
(1)	83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad
(1)	83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89
(1)	62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51
(1)	b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9
(1)	d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a
(1)	41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60
(1)	83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15
(1)	54:ee:44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26
(1)	dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad
(1)	a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01

172.17.50.100 (-, -) EqualLogic Device

Vulnerabilities (2)

■■■□□ 3 OpenSSH User Enumeration port 22/tcp

QID:	38737
Category:	General remote services
CVE ID:	CVE-2018-15473
Vendor Reference:	-
Bugtraq ID:	105140
Service Modified:	01/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

A username enumeration vulnerability exists in OpenSSH, that a remote attacker could leverage to enumerate valid users on a targeted system. The

attacker could try to enumerate users by transmitting malicious packets. Due to the vulnerability, if a username does not exist, then the server sends a SSH2_MSG_USERAUTH_FAILURE message to the attacker. If the username exists, then the server sends a SSH2_MSG_SERVICE_ACCEPT before calling fatal() and closes the connection.
In order for this vulnerability to be detected the "Password Brute Forcing" setting in the scan option profile needs to have a "System" value of "Standard" or higher.

IMPACT:

A remote attacker could check is a specific user account existed on the target server.

SOLUTION:

Upgrade to OpenSSH 7.8/7.8p1 or the latest version of openssh package for your operating system.
OpenSSH is available for download from OpenSSH's Web site (http://www.openssh.org/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.8/7.8p1: OpenSSH (https://www.openssh.com/releasenotes.html)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dreambox_openpli_shell
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/post/windows/gather/credentials/gpp
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/ssh/ssh_enumusers
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/plone_popen2
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dlink_dspw215_info_cgi_bof
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/docker_daemon_tcp
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/apache_roller_ognl_injection
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/http/ektron_cms400net
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/samba/chain_reply
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/post/windows/manage/ie_proxypac
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

The Exploit-DB

Reference:	CVE-2018-15473

Description: OpenSSH 2.3 < 7.7 - Username Enumeration - The Exploit-DB Ref : 45233
Link: http://www.exploit-db.com/exploits/45233

Reference: CVE-2018-15473
Description: OpenSSH < 7.7 - User Enumeration (2) - The Exploit-DB Ref : 45939
Link: http://www.exploit-db.com/exploits/45939

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) - The Exploit-DB Ref : 45210
Link: http://www.exploit-db.com/exploits/45210

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

root root

🟥🟥⬜⬜⬜ 2 Deprecated SSH Cryptographic Settings port 22/tcp

QID:	38739
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.
The target is using deprecated SSH cryptographic settings to communicate.

IMPACT:
A man-in-the-middle attacker may be able to exploit this vulnerability to record the communication to decrypt the session key and even the messages.

SOLUTION:
Avoid using deprecated cryptographic settings.
Use best practices when configuring SSH.
Refer to Security of Interactive and Automated Access Management Using Secure Shell (SSH) (https://csrc.nist.gov/publications/detail/nistir/7966/final) .
Settings currently considered deprecated:

Ciphers using CFB of OFB
Very uncommon, and deprecated because of weaknesses compared to newer cipher chaining modes such as CTR or GCM
RC4 cipher (arcfour, arcfour128, arcfour256)
The RC4 cipher has a cryptographic bias and is no longer considered secure
Ciphers with a 64-bit block size (DES, 3DES, Blowfish, IDEA, CAST)
Ciphers with a 64-bit block size may be vulnerable to birthday attacks (Sweet32)
Key exchange algorithms using DH group 1 (diffie-hellman-group1-sha1, gss-group1-sha1-*)
DH group 1 uses a 1024-bit key which is considered too short and vulnerable to Logjam-style attacks
Key exchange algorithm "rsa1024sha1"
Very uncommon, and deprecated because of the short RSA key size
MAC algorithm "umac-32"
Very uncommon, and deprecated because of the very short MAC length
Cipher "none"
This is available only in SSHv1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Type	Name
key exchange	diffie-hellman-group1-sha1

Potential Vulnerabilities (15)

■■■■□ 4 OpenSSH Multiple Vulnerabilities

QID:	38679
Category:	General remote services
CVE ID:	CVE-2015-5600, CVE-2015-6563, CVE-2015-6564
Vendor Reference:	OPENSSH 7.0
Bugtraq ID:	75990, 91787, 92012, 76317
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Multiple Vulnerabilities have been reported in OpenSSH.
- The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection. (CVE-2015-5600)
- The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests. (CVE-2015-6563)
- Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges. (CVE-2015-6564)
QID Detection Logic (Unauthenticated):
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:
Remote attackers could conduct brute-force attacks or cause a denial of service (CPU consumption).

SOLUTION:
OpenSSH 7.0 has been released to address this issue.
Update to the latest supported version of OpenSSH.
Check the OpenSSH 7.0 (http://www.openssh.com/txt/release-7.0) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OPENSSH 7.0: OpenSSH (http://www.openssh.com/txt/release-7.0)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■■□ 4 OpenSSH 7.4 Not Installed Multiple Vulnerabilities

QID:	38692
Category:	General remote services
CVE ID:	CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-8858
Vendor Reference:	OPENSSH 7.4
Bugtraq ID:	84312, 94968, 94972, 94977, 94975, 93776
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Multiple Vulnerabilities have been reported in OpenSSH v7.3 and earlier. These vulnerabilities if exploited will allow code execution, privilege escalation, information disclosure and denial of service attacks.
QID Detection Logic (Unauthenticated):
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Sucessful exploitation of the vulnerabilities will lead to code execution, privilege escalation, information disclosure and denial of service attacks.

SOLUTION:

OpenSSH 7.4 has been released to address this issue.
Update to the latest supported version of OpenSSH.
Check the OpenSSH 7.4 release notes page (http://www.openssh.com/txt/release-7.4) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OPENSSH 7.4 (http://www.openssh.com/txt/release-7.4)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2016-10010
Description:	OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation - The Exploit-DB Ref : 40962
Link:	http://www.exploit-db.com/exploits/40962
Reference:	CVE-2016-10009
Description:	OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading - The Exploit-DB Ref : 40963
Link:	http://www.exploit-db.com/exploits/40963

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Xauth Command Injection Vulnerability

QID:	38623
Category:	General remote services
CVE ID:	CVE-2016-3115
Vendor Reference:	OpenSSH 7.2p2
Bugtraq ID:	84314
Service Modified:	07/22/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The sshd server fails to validate user-supplied X11 authentication credentials when establishing an X11 forwarding session. An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie.
Please note that Systems with X11Forwarding enabled are affected.
Affected Versions:
OpenSSH versions prior to 7.2p2

IMPACT:

An authenticated, remote attacker can exploit this vulnerability to execute arbitrary commands on the targeted system.

SOLUTION:

Users are advised to upgrade to the latest version of the software available. Refer to OpenSSH 7.2p2 Release Notes (http://www.openssh.com/txt/release-7.2p2) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.2p2 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2016-3115
Description:	OpenSSH 7.2p1 - (Authenticated) xauth Command Injection - The Exploit-DB Ref : 39569
Link:	http://www.exploit-db.com/exploits/39569

Qualys

Reference:	CVE-2016-3115
Description:	OpenSSH
Link:	https://github.com/tintinweb/pub/tree/master/pocs/cve-2016-3115

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

3 OpenSSH Information Disclosure and Denial of Service Vulnerability

QID:	38725
Category:	General remote services
CVE ID:	CVE-2016-0777, CVE-2016-0778
Vendor Reference:	OpenSSH 7.1p2
Bugtraq ID:	80695, 80698
Service Modified:	08/05/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH contains the following vulnerabilities:
CVE-2016-0777: The resend_bytes function in roaming_common.c in the client allows remote attackers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
CVE-2016-0778: The roaming_read and roaming_write functions in roaming_common.c in the client when certain proxy and forward options are

enabled, do not properly maintain connection file descriptors, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.
Affected Versions:
OpenSSH 5.x, 6.x, and 7.x prior to 7.1p2
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation allows a remote attacker to gain access to sensitive information or cause a denial of service condition on the targeted system.

SOLUTION:

Customers are advised to upgrade to OpenSSH 7.1p2 (https://www.openssh.com/) or later to remediate these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.1p2 or later (https://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Qualys

Reference:	CVE-2016-0777
Description:	Qualys Security Advisory - Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778
Link:	http://seclists.org/fulldisclosure/2016/Jan/44

Reference:	CVE-2016-0778
Description:	Qualys Security Advisory - Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778
Link:	http://seclists.org/fulldisclosure/2016/Jan/44

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Username Enumeration Vulnerability

QID:	38726
Category:	General remote services
CVE ID:	CVE-2018-15473
Vendor Reference:	OpenBSDH OpenSSH
Bugtraq ID:	105140
Service Modified:	11/23/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
A username enumeration vulnerability exists in OpenSSH, that a remote attacker could leverage to enumerate valid users on a targeted system. The attacker could try to enumerate users by transmitting malicious packets. Due to the vulnerability, if a username does not exist, then the server sends a SSH2_MSG_USERAUTH_FAILURE message to the attacker. If the username exists, then the server sends a SSH2_MSG_SERVICE_ACCEPT before calling fatal() and closes the connection.
Affected Versions:
OpenSSH through 7.7
QID Detection Logic:
Authenticated: Vulnerable OpenSSH versions are detected by running ssh -V command.
Unauthenticated: Vulnerable OpenSSH versions are detected from the banner exposed.

IMPACT:

Successful exploitation allows an attacker to enumerate usernames on a targeted system.

SOLUTION:

Customers are advised to upgrade to OpenSSH 7.8 (https://www.openbsd.org/) or later versions to remediate this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.8 or later (https://www.openbsd.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dreambox_openpli_shell
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/gather/credentials/gpp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/ssh/ssh_enumusers
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/plone_popen2
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dlink_dspw215_info_cgi_bof
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/docker_daemon_tcp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/apache_roller_ognl_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/http/ektron_cms400net
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/samba/chain_reply
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/manage/ie_proxypac
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

The Exploit-DB

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration - The Exploit-DB Ref : 45233
Link: http://www.exploit-db.com/exploits/45233

Reference: CVE-2018-15473
Description: OpenSSH < 7.7 - User Enumeration (2) - The Exploit-DB Ref : 45939
Link: http://www.exploit-db.com/exploits/45939

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) - The Exploit-DB Ref : 45210
Link: http://www.exploit-db.com/exploits/45210

Qualys

Reference:	CVE-0000-0000
Description:	OpenSSH Username Enumeration
Link:	http://seclists.org/oss-sec/2018/q3/125

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Plaintext Recovery Attack Against SSH Vulnerability

QID:	42339
Category:	General remote services
CVE ID:	CVE-2008-5161
Vendor Reference:	openssh-5.2 release note
Bugtraq ID:	32319
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is prone to a plain text recovery attack. The issue is in the SSH protocol specification itself and exists in Secure Shell (SSH) software when used with CBC-mode ciphers.
Affected Versions:
OpenSSH Version 5.1 and earlier.

IMPACT:
This issue can be exploited by a remote unprivileged user to gain access to some of the plain text information from intercepted SSH network traffic, which would otherwise be encrypted.

SOLUTION:
Upgrade to OpenSSH 5.2 or later, available from the OpenSSH OpenSSH Download site (http://www.openssh.com/openbsd.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.2: OpenSSH (ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

■■■□□ 3 OpenSSH X11 Forwarding Information Disclosure

QID:	42378
Category:	General remote services
CVE ID:	CVE-2008-3259
Vendor Reference:	OpenSSH 5.1
Bugtraq ID:	30339
Service Modified:	07/17/2020
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is exposed to an information disclosure vulnerability caused by an error when binding to previously bound ports that have the SO_REUSEADDR option enabled and the sshd_config X11UseLocalhost option set to no.
Affected Versions:
OpenSSH Versions prior to 5.1 are vulnerable.

IMPACT:

Successfully exploiting this issue may allow an attacker to obtain sensitive information on systems where effective user-id or overlapping bind address checks are not present.

SOLUTION:

Upgrade to OpenSSH 5.1 or later, available from the OpenSSH OpenSSH 5.1 release notes (http://www.openssh.com/txt/release-5.1).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.1 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

🟨🟨🟨□□ 3 OpenSSH Commands Information Disclosure Vulnerability

QID:	42382
Category:	General remote services
CVE ID:	CVE-2012-0814
Vendor Reference:	OpenSSH Forced Command Information Disclosure
Bugtraq ID:	51702
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Openssh-server could allow a remote attacker to obtain sensitive information because of the improper handling of forced commands.

IMPACT:

Only authenticated users can exploit this vulnerability to obtain usernames and other sensitive information.

SOLUTION:

Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site (http://www.openssh.com/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.7 (OpenSSH) (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

■■■□□ 3 OpenSSH J-PAKE Session Key Retrieval Vulnerability

QID:	42384
Category:	General remote services
CVE ID:	CVE-2010-4478
Vendor Reference:	OpenSSH J-PAKE
Bugtraq ID:	45304
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol. This allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.
Affected Software:
OpenSSH versions 5.6 and prior.

IMPACT:
Successful exploitation allows attacker to get access to the remote system.

SOLUTION:
Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site (http://www.openssh.com/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH J-PAKE (http://www.openssh.com/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

■■■□□ 3 OpenSSH LoginGraceTime Denial of Service Vulnerability

QID:	42413
Category:	General remote services
CVE ID:	CVE-2010-5107
Vendor Reference:	OpenSSH
Bugtraq ID:	58162 , 58162
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Default OpenSSH installations have an overly long LoginGraceTime and a lack of early connection release for MaxStartups settings. Remote unauthenticated attackers could bypass the LoginGraceTime and MaxStartups thresholds by intermittently transmitting a large number of new TCP connections to the targeted server. This could lead to connection slot exhaustion.
Affected Software:
OpenSSH 6.1 and prior.

IMPACT:

Successful exploitation could allow an unauthenticated remote attacker to cause the targeted server to stop responding to legitimate user queries, leading to a denial of service on the targeted server.

SOLUTION:

Customers are advised to upgrade to OpenSSH 6.2 (http://www.openssh.org/) and apply the associated server configuration settings to remediate this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.2 (http://www.openssh.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 42413 detected on port 22 over TCP - SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

■■■□□ 3 Web Server Stopped Responding port 80/tcp

QID:	86476
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/28/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Web server stopped responding to 3 consecutive connection attempts and/or more than 3 consecutive HTTP / HTTPS requests. Consequently, the
service aborted testing for HTTP / HTTPS vulnerabilities. The vulnerabilities already detected are still posted.

IMPACT:

The service was unable to complete testing for HTTP / HTTPS vulnerabilities since the Web server stopped responding.

SOLUTION:

Check the Web server status.
If the Web server was crashed during the scan, please restart the server, report the incident to Customer Support and stop scanning the Web server until the issue is resolved.
If the Web server is unable to process multiple concurrent HTTP / HTTPS requests, please lower the scan harshness level and launch another scan.
If this vulnerability continues to be reported, please contact Customer Support.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
The web server did not respond for 4 consecutive HTTP requests.

■■■□□ 3 OpenSSH "X SECURITY" Bypass Vulnerability port 22/tcp

QID:	38611
Category:	General remote services
CVE ID:	CVE-2015-5352
Vendor Reference:	OpenSSH 6.9
Bugtraq ID:	75525
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

A vulnerability has been reported in the application which exist when using ssh -X option, to connect to the SSH client's X server which allow connections without being subject to X11 SECURITY restrictions.
Affected Versions:
OpenSSH prior to version 6.9

IMPACT:
Succesful exploitation of this vulnerability will allow an attacker to interact with X server without being subject to X SECURITY restrictions or authentication

SOLUTION:
Users are advised to upgrade to the latest version of the software available. Refer to OpenSSH 6.9 Release Notes (http://www.openssh.org/txt/release-6.9) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.9 (http://www.openssh.com/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■□□□ 2 OpenSSH Information Disclosure Vulnerability

QID:	38788
Category:	General remote services
CVE ID:	CVE-2011-4327
Vendor Reference:	Openssh
Bugtraq ID:	-
Service Modified:	01/12/2021
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.
Affected Versions:
OpenSSH before 5.8p2
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation could disclose sensitive information.

SOLUTION:

Customers are advised to upgrade to OpenSSH 5.8p2 (http://www.openssh.com/txt/portable-keysign-rand-helper.adv) or later to remediate these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2011-4327 (http://www.openssh.com/txt/portable-keysign-rand-helper.adv)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■□□□ 2 OpenSSH "child_set_env()" Security Bypass Issue

QID:	42428
Category:	General remote services
CVE ID:	CVE-2014-2532
Vendor Reference:	OpenSSH 6.6
Bugtraq ID:	66355
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The security issue is caused by an error within the "child_set_env()" function (usr.bin/ssh/session.c) and can be exploited to bypass intended environment restrictions by using a substring before a wildcard character.
Affected Versions:
OpenSSH Versions prior to 6.6 are affected

IMPACT:

This issue can be exploited by malicious local users to bypass certain security restrictions.

SOLUTION:

Upgrade to OpenSSH 6.6 or later to resolve this issue. Refer to OpenSSH 6.6 Release Notes (http://www.openssh.org/txt/release-6.6) for further

information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.6: OpenSSH (http://www.openssh.org/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

🟨🟨□□□ 2 Global User List Found Using Other QIDS

QID:	45002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/16/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities or via authentication provided by user. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.
Note: We did not exploit any vulnerabilities to gather this information in QID 90266, 45027 or 45032.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	Source Vulnerability (QualysID)
root	38737

Information Gathered (15)

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/23/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Service name: SNMP on UDP port 161.
Service name: SSH on TCP port 22.

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the

fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
EqualLogic Device	TCP/IP Fingerprint	U4444:22

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.50.100	No registered hostname

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
4,6,8,10,12,14,16,26,28,30,32,34,36,40,224-241,247-255,266-279,283-308,
310,312-317,319-321,326-341,343,352-362,364-368,582-586,588-591,594-597,
599,601-605,621-623,625-626,628-630,632,638-665,675-699,701-703,706,708,
712-728,732,734-739,743,745-746,755-757,766,768,778-779,784-785,787-798,
802-809,811-859,861-872,874-885,889-899,902-910,913-949,951-953,956-973,
975-989,994,1002-1007,1009,1012-1014,1016-1022,1101-1108,1113,1115,1117-1122,
1124-1154,1156-1166,1168-1169,1171-1206,1208-1211,1213,1215-1219,1223-1233,
1237-1240,1242,1244,1246-1247,1249-1268,1270-1287,1289-1312,1315-1336,
1338-1343,1626-1635,1775,1816-1817,1825-1877,1879-1899,1910,1921, and more.
We have omitted from this list 61905 higher ports to keep the report size manageable.
```

■□□□□ 1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	172.17.1.1	8.81ms	UDP	80
2	172.17.50.100	3.77ms	ICMP	

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2382 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:16:49 GMT

1 Scan Activity per Port

QID:	45426
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	22	0:06:28
TCP	80	0:38:21
TCP	3002	0:07:34
TCP	9876	0:00:32
UDP	123	0:01:24
UDP	161	0:03:12

■□□□□ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	ntp
161	snmp	SNMP	snmp

▮▯▯▯▯ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www-http	World Wide Web HTTP	http	
3002	remoteware-srv	RemoteWare Server	unknown	
3260	unknown	unknown	iSCSI	

9876	sd	Session Director	unknown

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 1054	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 43439	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 512	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 51100	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 135	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1981	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1434	Port Unreachable

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1042321734 with a standard deviation of 556730880. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5113 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 22: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 4 6 6 9 9
Duration: 26 milli seconds

■□□□□ 1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

■□□□□ 1 SSH daemon information retrieving port 22/tcp

QID:	38047
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

```
For Red Hat ES 4:-
SSH1 supported                                                    yes
Supported authentification methods for SSH1              RSA,password
Supported ciphers for SSH1                                    3des,blowfish
SSH2 supported                                                    yes
Supported keys exchange algorithm for SSH2              diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-
sha1
Supported decryption ciphers for SSH2                         aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,
rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2                         aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,
rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2                          hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
```

hmac-md5-96
Supported encryption mac for SSH2 hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96
Supported authentification methods for SSH2 publickey,gssapi-with-mic,password

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
Supported host key algorithms for SSH2	ssh-rsa
Supported decryption ciphers for SSH2	aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
Supported decryption macs for SSH2	hmac-sha1, hmac-sha1-96
Supported encryption macs for SSH2	hmac-sha1, hmac-sha1-96
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, password

■□□□□ 1 SSH Banner port 22/tcp

QID:	38050
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/30/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.
QID Detection Logic:
The QID checks for SSH in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

172.17.50.101 (-, -) IBM OS/400 on AS/400

Vulnerabilities (2)

🟥🟥🟥⬜⬜ 3 OpenSSH User Enumeration port 22/tcp

QID:	38737
Category:	General remote services
CVE ID:	CVE-2018-15473
Vendor Reference:	-
Bugtraq ID:	105140
Service Modified:	01/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
A username enumeration vulnerability exists in OpenSSH, that a remote attacker could leverage to enumerate valid users on a targeted system. The attacker could try to enumerate users by transmitting malicious packets. Due to the vulnerability, if a username does not exist, then the server sends a SSH2_MSG_USERAUTH_FAILURE message to the attacker. If the username exists, then the server sends a SSH2_MSG_SERVICE_ACCEPT before calling fatal() and closes the connection.
In order for this vulnerability to be detected the "Password Brute Forcing" setting in the scan option profile needs to have a "System" value of "Standard" or higher.

IMPACT:
A remote attacker could check is a specific user account existed on the target server.

SOLUTION:
Upgrade to OpenSSH 7.8/7.8p1 or the latest version of openssh package for your operating system.
OpenSSH is available for download from OpenSSH's Web site (http://www.openssh.org/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.8/7.8p1: OpenSSH (https://www.openssh.com/releasenotes.html)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
Metasploit

Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dreambox_openpli_shell
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb
Reference:	CVE-2018-15473
Description:	SSH Username Enumeration - Metasploit Ref : /modules/post/windows/gather/credentials/gpp
Link:	https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/ssh/ssh_enumusers
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/plone_popen2
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dlink_dspw215_info_cgi_bof
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/docker_daemon_tcp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/apache_roller_ognl_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/http/ektron_cms400net
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/samba/chain_reply
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/manage/ie_proxypac
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

The Exploit-DB

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration - The Exploit-DB Ref : 45233
Link: http://www.exploit-db.com/exploits/45233

Reference: CVE-2018-15473
Description: OpenSSH < 7.7 - User Enumeration (2) - The Exploit-DB Ref : 45939
Link: http://www.exploit-db.com/exploits/45939

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) - The Exploit-DB Ref : 45210
Link: http://www.exploit-db.com/exploits/45210

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

root root

🟥🟥□□□ 2 Deprecated SSH Cryptographic Settings port 22/tcp

QID:	38739
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/03/2019
User Modified:	-
Edited:	No

PCI Vuln:	Yes

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.
The target is using deprecated SSH cryptographic settings to communicate.

IMPACT:

A man-in-the-middle attacker may be able to exploit this vulnerability to record the communication to decrypt the session key and even the messages.

SOLUTION:

Avoid using deprecated cryptographic settings.
Use best practices when configuring SSH.
Refer to Security of Interactive and Automated Access Management Using Secure Shell (SSH) (https://csrc.nist.gov/publications/detail/nistir/7966/final) .
Settings currently considered deprecated:

Ciphers using CFB of OFB
Very uncommon, and deprecated because of weaknesses compared to newer cipher chaining modes such as CTR or GCM
RC4 cipher (arcfour, arcfour128, arcfour256)
The RC4 cipher has a cryptographic bias and is no longer considered secure
Ciphers with a 64-bit block size (DES, 3DES, Blowfish, IDEA, CAST)
Ciphers with a 64-bit block size may be vulnerable to birthday attacks (Sweet32)
Key exchange algorithms using DH group 1 (diffie-hellman-group1-sha1, gss-group1-sha1-*)
DH group 1 uses a 1024-bit key which is considered too short and vulnerable to Logjam-style attacks
Key exchange algorithm "rsa1024sha1"
Very uncommon, and deprecated because of the short RSA key size
MAC algorithm "umac-32"
Very uncommon, and deprecated because of the very short MAC length
Cipher "none"
This is available only in SSHv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Type	Name
key exchange	diffie-hellman-group1-sha1

Potential Vulnerabilities (15)

■■■■□ 4 OpenSSH Multiple Vulnerabilities

QID:	38679
Category:	General remote services
CVE ID:	CVE-2015-5600, CVE-2015-6563, CVE-2015-6564
Vendor Reference:	OPENSSH 7.0
Bugtraq ID:	75990, 91787, 92012, 76317
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Multiple Vulnerabilities have been reported in OpenSSH.
- The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection. (CVE-2015-5600)
- The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests. (CVE-2015-6563)
- Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges. (CVE-2015-6564)

QID Detection Logic (Unauthenticated):
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Remote attackers could conduct brute-force attacks or cause a denial of service (CPU consumption).

SOLUTION:

OpenSSH 7.0 has been released to address this issue.
Update to the latest supported version of OpenSSH.
Check the OpenSSH 7.0 (http://www.openssh.com/txt/release-7.0) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OPENSSH 7.0: OpenSSH (http://www.openssh.com/txt/release-7.0)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■■□ 4 OpenSSH 7.4 Not Installed Multiple Vulnerabilities

QID:	38692
Category:	General remote services
CVE ID:	CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-8858
Vendor Reference:	OPENSSH 7.4
Bugtraq ID:	84312, 94968, 94972, 94977, 94975, 93776
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Multiple Vulnerabilities have been reported in OpenSSH v7.3 and earlier. These vulnerabilities if exploited will allow code execution, privilege escalation, information disclosure and denial of service attacks.
QID Detection Logic (Unauthenticated):
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Sucessful exploitation of the vulnerabilities will lead to code execution, privilege escalation, information disclosure and denial of service attacks.

SOLUTION:

OpenSSH 7.4 has been released to address this issue.
Update to the latest supported version of OpenSSH.
Check the OpenSSH 7.4 release notes page (http://www.openssh.com/txt/release-7.4) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OPENSSH 7.4 (http://www.openssh.com/txt/release-7.4)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
The Exploit-DB

Reference:	CVE-2016-10010
Description:	OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation - The Exploit-DB Ref : 40962
Link:	http://www.exploit-db.com/exploits/40962
Reference:	CVE-2016-10009
Description:	OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading - The Exploit-DB Ref : 40963
Link:	http://www.exploit-db.com/exploits/40963

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

3 OpenSSH Xauth Command Injection Vulnerability

QID:	38623
Category:	General remote services
CVE ID:	CVE-2016-3115
Vendor Reference:	OpenSSH 7.2p2
Bugtraq ID:	84314
Service Modified:	07/22/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The sshd server fails to validate user-supplied X11 authentication credentials when establishing an X11 forwarding session. An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie.
Please note that Systems with X11Forwarding enabled are affected.
Affected Versions:
OpenSSH versions prior to 7.2p2

IMPACT:
An authenticated, remote attacker can exploit this vulnerability to execute arbitrary commands on the targeted system.

SOLUTION:
Users are advised to upgrade to the latest version of the software available. Refer to OpenSSH 7.2p2 Release Notes (http://www.openssh.com/txt/release-7.2p2) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.2p2 (http://www.openssh.com/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
The Exploit-DB

Reference:	CVE-2016-3115
Description:	OpenSSH 7.2p1 - (Authenticated) xauth Command Injection - The Exploit-DB Ref : 39569
Link:	http://www.exploit-db.com/exploits/39569

Qualys

Reference:	CVE-2016-3115
Description:	OpenSSH
Link:	https://github.com/tintinweb/pub/tree/master/pocs/cve-2016-3115

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Information Disclosure and Denial of Service Vulnerability

QID:	38725
Category:	General remote services
CVE ID:	CVE-2016-0777, CVE-2016-0778
Vendor Reference:	OpenSSH 7.1p2
Bugtraq ID:	80695, 80698
Service Modified:	08/05/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH contains the following vulnerabilities:
CVE-2016-0777: The resend_bytes function in roaming_common.c in the client allows remote attackers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
CVE-2016-0778: The roaming_read and roaming_write functions in roaming_common.c in the client when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.
Affected Versions:
OpenSSH 5.x, 6.x, and 7.x prior to 7.1p2
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation allows a remote attacker to gain access to sensitive information or cause a denial of service condition on the targeted system.

SOLUTION:

Customers are advised to upgrade to OpenSSH 7.1p2 (https://www.openssh.com/) or later to remediate these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.1p2 or later (https://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Qualys

Reference:	CVE-2016-0777
Description:	Qualys Security Advisory - Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778
Link:	http://seclists.org/fulldisclosure/2016/Jan/44

Reference:	CVE-2016-0778
Description:	Qualys Security Advisory - Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778
Link:	http://seclists.org/fulldisclosure/2016/Jan/44

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Username Enumeration Vulnerability

QID:	38726
Category:	General remote services
CVE ID:	CVE-2018-15473
Vendor Reference:	OpenBSDH OpenSSH
Bugtraq ID:	105140
Service Modified:	11/23/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
A username enumeration vulnerability exists in OpenSSH, that a remote attacker could leverage to enumerate valid users on a targeted system. The attacker could try to enumerate users by transmitting malicious packets. Due to the vulnerability, if a username does not exist, then the server sends a SSH2_MSG_USERAUTH_FAILURE message to the attacker. If the username exists, then the server sends a SSH2_MSG_SERVICE_ACCEPT before calling fatal() and closes the connection.
Affected Versions:
OpenSSH through 7.7
QID Detection Logic:
Authenticated: Vulnerable OpenSSH versions are detected by running ssh -V command.
Unauthenticated: Vulnerable OpenSSH versions are detected from the banner exposed.

IMPACT:

Successful exploitation allows an attacker to enumerate usernames on a targeted system.

SOLUTION:

Customers are advised to upgrade to OpenSSH 7.8 (https://www.openbsd.org/) or later versions to remediate this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.8 or later (https://www.openbsd.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dreambox_openpli_shell
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/gather/credentials/gpp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/ssh/ssh_enumusers
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/plone_popen2
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dlink_dspw215_info_cgi_bof

Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/docker_daemon_tcp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/apache_roller_ognl_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/http/ektron_cms400net
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/samba/chain_reply
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/manage/ie_proxypac
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

The Exploit-DB

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration - The Exploit-DB Ref : 45233
Link: http://www.exploit-db.com/exploits/45233

Reference: CVE-2018-15473
Description: OpenSSH < 7.7 - User Enumeration (2) - The Exploit-DB Ref : 45939
Link: http://www.exploit-db.com/exploits/45939

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) - The Exploit-DB Ref : 45210
Link: http://www.exploit-db.com/exploits/45210

Qualys

Reference: CVE-0000-0000
Description: OpenSSH Username Enumeration
Link: http://seclists.org/oss-sec/2018/q3/125

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Plaintext Recovery Attack Against SSH Vulnerability

QID:	42339
Category:	General remote services
CVE ID:	CVE-2008-5161
Vendor Reference:	openssh-5.2 release note
Bugtraq ID:	32319
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is prone to a plain text recovery attack. The issue is in the SSH protocol specification itself and exists in Secure Shell (SSH) software when used with CBC-mode ciphers.
Affected Versions:
OpenSSH Version 5.1 and earlier.

IMPACT:

This issue can be exploited by a remote unprivileged user to gain access to some of the plain text information from intercepted SSH network traffic, which would otherwise be encrypted.

SOLUTION:

Upgrade to OpenSSH 5.2 or later, available from the OpenSSH OpenSSH Download site (http://www.openssh.com/openbsd.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.2: OpenSSH (ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

🟨🟨🟨□□ 3 OpenSSH X11 Forwarding Information Disclosure

QID:	42378
Category:	General remote services
CVE ID:	CVE-2008-3259
Vendor Reference:	OpenSSH 5.1
Bugtraq ID:	30339
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is exposed to an information disclosure vulnerability caused by an error when binding to previously bound ports that have the SO_REUSEADDR option enabled and the sshd_config X11UseLocalhost option set to no.
Affected Versions:
OpenSSH Versions prior to 5.1 are vulnerable.

IMPACT:

Successfully exploiting this issue may allow an attacker to obtain sensitive information on systems where effective user-id or overlapping bind address checks are not present.

SOLUTION:

Upgrade to OpenSSH 5.1 or later, available from the OpenSSH OpenSSH 5.1 release notes (http://www.openssh.com/txt/release-5.1).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.1 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

■■■□□ 3 OpenSSH Commands Information Disclosure Vulnerability

QID:	42382
Category:	General remote services
CVE ID:	CVE-2012-0814
Vendor Reference:	OpenSSH Forced Command Information Disclosure
Bugtraq ID:	51702
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Openssh-server could allow a remote attacker to obtain sensitive information because of the improper handling of forced commands.

IMPACT:

Only authenticated users can exploit this vulnerability to obtain usernames and other sensitive information.

SOLUTION:

Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site (http://www.openssh.com/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.7 (OpenSSH) (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

■■■□□ 3 OpenSSH J-PAKE Session Key Retrieval Vulnerability

QID:	42384
Category:	General remote services
CVE ID:	CVE-2010-4478
Vendor Reference:	OpenSSH J-PAKE
Bugtraq ID:	45304
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol. This allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.
Affected Software:

OpenSSH versions 5.6 and prior.

IMPACT:
Successful exploitation allows attacker to get access to the remote system.

SOLUTION:
Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site (http://www.openssh.com/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH J-PAKE (http://www.openssh.com/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

■■■□□ 3 OpenSSH LoginGraceTime Denial of Service Vulnerability

QID:	42413
Category:	General remote services
CVE ID:	CVE-2010-5107
Vendor Reference:	OpenSSH
Bugtraq ID:	58162 , 58162
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Default OpenSSH installations have an overly long LoginGraceTime and a lack of early connection release for MaxStartups settings. Remote unauthenticated attackers could bypass the LoginGraceTime and MaxStartups thresholds by intermittently transmitting a large number of new TCP connections to the targeted server. This could lead to connection slot exhaustion.
Affected Software:
OpenSSH 6.1 and prior.

IMPACT:
Successful exploitation could allow an unauthenticated remote attacker to cause the targeted server to stop responding to legitimate user queries, leading to a denial of service on the targeted server.

SOLUTION:
Customers are advised to upgrade to OpenSSH 6.2 (http://www.openssh.org/) and apply the associated server configuration settings to remediate this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.2 (http://www.openssh.org/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 42413 detected on port 22 over TCP - SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

■■■□□ 3 OpenSSH "X SECURITY" Bypass Vulnerability port 22/tcp

QID:	38611
Category:	General remote services
CVE ID:	CVE-2015-5352
Vendor Reference:	OpenSSH 6.9
Bugtraq ID:	75525
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

A vulnerability has been reported in the application which exist when using ssh -X option, to connect to the SSH client's X server which allow connections without being subject to X11 SECURITY restrictions.
Affected Versions:
OpenSSH prior to version 6.9

IMPACT:

Succesful exploitation of this vulnerability will allow an attacker to interact with X server without being subject to X SECURITY restrictions or authentication

SOLUTION:

Users are advised to upgrade to the latest version of the software available. Refer to OpenSSH 6.9 Release Notes (http://www.openssh.org/txt/release-6.9) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.9 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 Service Stopped Responding port 3002/tcp

QID:	38229
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/12/2009
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The service/daemon listening on the port shown stopped responding to TCP connection attempts during the scan.

IMPACT:

The service/daemon is vulnerable to a denial of service attack.

SOLUTION:

This QID can be posted for a number of reasons (e.g., service crash, bandwidth utilization, or a device with IPS-like behavior).
If the service has crashed, report the incident to Customer Support or your QualysGuard re-seller, and stop scanning the service's listening port until the issue is resolved.
If the issue is bandwidth related, modify the Qualys performance settings to lower the scan impact.
If you do not find any service/daemon listening on this port, it may be a dynamic port and you may ignore this report.
This is posted as a PCI fail since the service stopped responding. Further checks were not launched for that service and therefore the PCI assessment was incomplete.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

3 consecutive connection attempts failed after a total number of 42 successful connections.

■■□□□ 2 OpenSSH Information Disclosure Vulnerability

QID:	38788
Category:	General remote services
CVE ID:	CVE-2011-4327
Vendor Reference:	Openssh
Bugtraq ID:	-
Service Modified:	01/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.
Affected Versions:
OpenSSH before 5.8p2
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation could disclose sensitive information.

SOLUTION:

Customers are advised to upgrade to OpenSSH 5.8p2 (http://www.openssh.com/txt/portable-keysign-rand-helper.adv) or later to remediate these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2011-4327 (http://www.openssh.com/txt/portable-keysign-rand-helper.adv)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

🟨🟨⬜⬜⬜ 2 OpenSSH "child_set_env()" Security Bypass Issue

QID:	42428
Category:	General remote services
CVE ID:	CVE-2014-2532
Vendor Reference:	OpenSSH 6.6
Bugtraq ID:	66355
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The security issue is caused by an error within the "child_set_env()" function (usr.bin/ssh/session.c) and can be exploited to bypass intended environment restrictions by using a substring before a wildcard character.
Affected Versions:
OpenSSH Versions prior to 6.6 are affected

IMPACT:
This issue can be exploited by malicious local users to bypass certain security restrictions.

SOLUTION:
Upgrade to OpenSSH 6.6 or later to resolve this issue. Refer to OpenSSH 6.6 Release Notes (http://www.openssh.org/txt/release-6.6) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.6: OpenSSH (http://www.openssh.org/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

🟨🟨⬜⬜⬜ 2 Global User List Found Using Other QIDS

QID:	45002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/16/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities or via authentication provided by user. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.
Note: We did not exploit any vulnerabilities to gather this information in QID 90266, 45027 or 45032.

IMPACT:

These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:

To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

User Name	Source Vulnerability (QualysID)
root	38737

Information Gathered (16)

■■■□□ 3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/23/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Service name: SNMP on UDP port 161.
Service name: SSH on TCP port 22.

■■■□□ 3 Exhaustive Web Testing Skipped port 80/tcp

QID:	86718
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/13/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The service aborted the scanning of the Web server before completion, since the Web server stopped responding to HTTP requests during the course
of scanning. The service attempted to reconnect to the Web server two minutes later and found it responsive again. However, the service has chosen to stop further scanning of the Web server to avoid possible interruption of the Web service.

IMPACT:

Since the service did not complete scanning this host, not all vulnerability tests were completed. It's possible that not all vulnerabilities were detected for this host.

SOLUTION:

There may have been a number of conditions that contributed to this issue. The following is a partial list of possibilities that should be investigated:
- The Web server may have reached its connection limit.
- The Web server (or an intervening network device) may have been purposefully throttling connections (e.g. mod_throttle for Apache).
- The Web server (or an intervening network device) may contain an undisclosed Denial of Service condition that was triggered by the scan traffic.
- The Web server (or an intervening network device) may have experienced a degradation of performance due to high load (e.g. via scanning multiple virtual

IPs on the same physical host).
- The scan traffic may have been traversing a network segment with limited bandwidth capacity.
- An Intrusion Prevention System, reactive firewall, or similar device may have detected and blocked the scan traffic.
This issue may possibly be mitigated by modifying the scan performance settings in your option profile before scanning the host again.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

The web server stopped responding to 4 consecutive HTTP requests 2 minutes ago. Although it resumed responding to a new HTTP request but the service had terminated further scanning of the web server to avoid interrupting the web server's normal functionality and a prolonged scanning time.

2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
IBM OS/400 on AS/400	TCP/IP Fingerprint	U4444:80

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.50.101	No registered hostname

■□□□□ 1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Some of the ports filtered by the firewall are: 11, 67, 79, 1723, 2049, 2764, 2869.
Firewall responded to TCP probes sent to port 135 with RST packets (hopcount to firewall 1 vs hopcount to target 2).

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
4,6,8,10,12,14,16,26,28,30,32,34,36,40,224-241,247-255,266-279,283-308,
310,312-317,319-321,326-343,352-362,364-368,582-584,586,588-591,594-597,
599,601-605,621-623,625-626,628-630,632,638-647,649-665,675-699,701-703,
706,708,712-713,715-728,732-737,739,743,745-746,755-757,766,768,778-779,
```

784-785,787,789-798,802-832,834-859,861-872,874-885,889-899,902-910,913-949,
951-953,956-989,994,1002-1007,1009,1012-1014,1016-1022,1101-1108,1113,
1115-1121,1124-1154,1156-1166,1168-1169,1171-1206,1208-1211,1213,1215-1219,
1223-1233,1237-1240,1242,1244,1246-1247,1249-1261,1263-1268,1270-1300,
1302-1312,1315-1336,1338-1343,1626-1635,1775,1816-1817,1825-1899,1910, and more.
We have omitted from this list 61881 higher ports to keep the report size manageable.

▮□□□□ 1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	172.17.1.1	6.48ms	ICMP	
2	172.17.50.101	3.25ms	TCP	80

▮□□□□ 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2468 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:18:15 GMT

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	22	0:05:32
TCP	80	1:00:09
TCP	3002	0:04:32
TCP	9876	0:00:32
UDP	123	0:01:24

UDP	161	0:03:12

■□□□□ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	ntp
161	snmp	SNMP	snmp

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www-http	World Wide Web HTTP	http	
3002	remoteware-srv	RemoteWare Server	unknown	
3260	unknown	unknown	iSCSI	
9876	sd	Session Director	unknown	

▮▯▯▯▯ 1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information

Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 1054	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 512	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 18912	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 51100	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 135	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1981	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1434	Port Unreachable

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1172899300 with a standard deviation of 667486815. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5110 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
IP ID changes observed (network order) for port 22: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 3 5
Duration: 29 milli seconds
```

1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

1 SSH daemon information retrieving port 22/tcp

QID:	38047

Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

For Red Hat ES 4:-

SSH1 supported	yes
Supported authentification methods for SSH1	RSA,password
Supported ciphers for SSH1	3des,blowfish
SSH2 supported	yes
Supported keys exchange algorithm for SSH2	diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported encryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported authentification methods for SSH2	publickey,gssapi-with-mic,password

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
Supported host key algorithms for SSH2	ssh-rsa
Supported decryption ciphers for SSH2	aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
Supported decryption macs for SSH2	hmac-sha1, hmac-sha1-96
Supported encryption macs for SSH2	hmac-sha1, hmac-sha1-96
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, password

■□□□□ 1 SSH Banner port 22/tcp

QID:	38050
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/30/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.
QID Detection Logic:
The QID checks for SSH in the banner of the response.

IMPACT:
NA

SOLUTION:
NA

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

172.17.50.102 (-, -) EqualLogic Device

Vulnerabilities (2)

■■■□□ 3 OpenSSH User Enumeration port 22/tcp

QID:	38737
Category:	General remote services
CVE ID:	CVE-2018-15473
Vendor Reference:	-
Bugtraq ID:	105140
Service Modified:	01/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
A username enumeration vulnerability exists in OpenSSH, that a remote attacker could leverage to enumerate valid users on a targeted system. The attacker could try to enumerate users by transmitting malicious packets. Due to the vulnerability, if a username does not exist, then the server sends a SSH2_MSG_USERAUTH_FAILURE message to the attacker. If the username exists, then the server sends a SSH2_MSG_SERVICE_ACCEPT before calling fatal() and closes the connection.
In order for this vulnerability to be detected the "Password Brute Forcing" setting in the scan option profile needs to have a "System" value of "Standard" or higher.

IMPACT:
A remote attacker could check is a specific user account existed on the target server.

SOLUTION:
Upgrade to OpenSSH 7.8/7.8p1 or the latest version of openssh package for your operating system.
OpenSSH is available for download from OpenSSH's Web site (http://www.openssh.org/).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.8/7.8p1: OpenSSH (https://www.openssh.com/releasenotes.html)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dreambox_openpli_shell
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/gather/credentials/gpp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/ssh/ssh_enumusers
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/plone_popen2
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dlink_dspw215_info_cgi_bof
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/docker_daemon_tcp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/apache_roller_ognl_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/http/ektron_cms400net
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/samba/chain_reply
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/manage/ie_proxypac
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

The Exploit-DB

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration - The Exploit-DB Ref : 45233
Link: http://www.exploit-db.com/exploits/45233

Reference: CVE-2018-15473

Description: OpenSSH < 7.7 - User Enumeration (2) - The Exploit-DB Ref : 45939
Link: http://www.exploit-db.com/exploits/45939

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) - The Exploit-DB Ref : 45210
Link: http://www.exploit-db.com/exploits/45210

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
root root

🟥🟥□□□ 2 Deprecated SSH Cryptographic Settings port 22/tcp

QID:	38739
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another.
The target is using deprecated SSH cryptographic settings to communicate.

IMPACT:
A man-in-the-middle attacker may be able to exploit this vulnerability to record the communication to decrypt the session key and even the messages.

SOLUTION:
Avoid using deprecated cryptographic settings.
Use best practices when configuring SSH.
Refer to Security of Interactive and Automated Access Management Using Secure Shell (SSH) (https://csrc.nist.gov/publications/detail/nistir/7966/final) .
Settings currently considered deprecated:

Ciphers using CFB of OFB
Very uncommon, and deprecated because of weaknesses compared to newer cipher chaining modes such as CTR or GCM
RC4 cipher (arcfour, arcfour128, arcfour256)
The RC4 cipher has a cryptographic bias and is no longer considered secure
Ciphers with a 64-bit block size (DES, 3DES, Blowfish, IDEA, CAST)
Ciphers with a 64-bit block size may be vulnerable to birthday attacks (Sweet32)
Key exchange algorithms using DH group 1 (diffie-hellman-group1-sha1, gss-group1-sha1-*)
DH group 1 uses a 1024-bit key which is considered too short and vulnerable to Logjam-style attacks
Key exchange algorithm "rsa1024sha1"
Very uncommon, and deprecated because of the short RSA key size
MAC algorithm "umac-32"
Very uncommon, and deprecated because of the very short MAC length
Cipher "none"
This is available only in SSHv1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Type	Name
key exchange	diffie-hellman-group1-sha1

Potential Vulnerabilities (15)

4 OpenSSH Multiple Vulnerabilities

QID:	38679
Category:	General remote services
CVE ID:	CVE-2015-5600, CVE-2015-6563, CVE-2015-6564
Vendor Reference:	OPENSSH 7.0
Bugtraq ID:	75990, 91787, 92012, 76317
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Multiple Vulnerabilities have been reported in OpenSSH.
- The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection. (CVE-2015-5600)
- The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests. (CVE-2015-6563)
- Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges. (CVE-2015-6564)

QID Detection Logic (Unauthenticated):
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Remote attackers could conduct brute-force attacks or cause a denial of service (CPU consumption).

SOLUTION:

OpenSSH 7.0 has been released to address this issue.
Update to the latest supported version of OpenSSH.
Check the OpenSSH 7.0 (http://www.openssh.com/txt/release-7.0) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OPENSSH 7.0: OpenSSH (http://www.openssh.com/txt/release-7.0)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

4 OpenSSH 7.4 Not Installed Multiple Vulnerabilities

QID:	38692
Category:	General remote services
CVE ID:	CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-8858

Vendor Reference:	OPENSSH 7.4
Bugtraq ID:	84312, 94968, 94972, 94977, 94975, 93776
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Multiple Vulnerabilities have been reported in OpenSSH v7.3 and earlier. These vulnerabilities if exploited will allow code execution, privilege escalation, information disclosure and denial of service attacks.
QID Detection Logic (Unauthenticated):
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Sucessful exploitation of the vulnerabilities will lead to code execution, privilege escalation, information disclosure and denial of service attacks.

SOLUTION:

OpenSSH 7.4 has been released to address this issue.
Update to the latest supported version of OpenSSH.
Check the OpenSSH 7.4 release notes page (http://www.openssh.com/txt/release-7.4) for further information.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OPENSSH 7.4 (http://www.openssh.com/txt/release-7.4)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2016-10010
Description:	OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation - The Exploit-DB Ref : 40962
Link:	http://www.exploit-db.com/exploits/40962
Reference:	CVE-2016-10009
Description:	OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading - The Exploit-DB Ref : 40963
Link:	http://www.exploit-db.com/exploits/40963

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Xauth Command Injection Vulnerability

QID:	38623
Category:	General remote services
CVE ID:	CVE-2016-3115
Vendor Reference:	OpenSSH 7.2p2
Bugtraq ID:	84314
Service Modified:	07/22/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The sshd server fails to validate user-supplied X11 authentication credentials when establishing an X11 forwarding session. An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie.
Please note that Systems with X11Forwarding enabled are affected.
Affected Versions:
OpenSSH versions prior to 7.2p2

IMPACT:

An authenticated, remote attacker can exploit this vulnerability to execute arbitrary commands on the targeted system.

SOLUTION:

Users are advised to upgrade to the latest version of the software available. Refer to OpenSSH 7.2p2 Release Notes (http://www.openssh.com/txt/release-7.2p2) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.2p2 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

The Exploit-DB

Reference:	CVE-2016-3115
Description:	OpenSSH 7.2p1 - (Authenticated) xauth Command Injection - The Exploit-DB Ref : 39569
Link:	http://www.exploit-db.com/exploits/39569

Qualys

Reference:	CVE-2016-3115
Description:	OpenSSH
Link:	https://github.com/tintinweb/pub/tree/master/pocs/cve-2016-3115

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Information Disclosure and Denial of Service Vulnerability

QID:	38725
Category:	General remote services
CVE ID:	CVE-2016-0777, CVE-2016-0778
Vendor Reference:	OpenSSH 7.1p2
Bugtraq ID:	80695, 80698
Service Modified:	08/05/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH contains the following vulnerabilities:
CVE-2016-0777: The resend_bytes function in roaming_common.c in the client allows remote attackers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
CVE-2016-0778: The roaming_read and roaming_write functions in roaming_common.c in the client when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.
Affected Versions:
OpenSSH 5.x, 6.x, and 7.x prior to 7.1p2
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation allows a remote attacker to gain access to sensitive information or cause a denial of service condition on the targeted system.

SOLUTION:

Customers are advised to upgrade to OpenSSH 7.1p2 (https://www.openssh.com/) or later to remediate these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.1p2 or later (https://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Qualys

Reference:	CVE-2016-0777
Description:	Qualys Security Advisory - Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778
Link:	http://seclists.org/fulldisclosure/2016/Jan/44

Reference:	CVE-2016-0778
Description:	Qualys Security Advisory - Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778
Link:	http://seclists.org/fulldisclosure/2016/Jan/44

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Username Enumeration Vulnerability

QID:	38726
Category:	General remote services
CVE ID:	CVE-2018-15473
Vendor Reference:	OpenBSDH OpenSSH
Bugtraq ID:	105140
Service Modified:	11/23/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
A username enumeration vulnerability exists in OpenSSH, that a remote attacker could leverage to enumerate valid users on a targeted system. The attacker could try to enumerate users by transmitting malicious packets. Due to the vulnerability, if a username does not exist, then the server sends a SSH2_MSG_USERAUTH_FAILURE message to the attacker. If the username exists, then the server sends a SSH2_MSG_SERVICE_ACCEPT before calling fatal() and closes the connection.
Affected Versions:
OpenSSH through 7.7
QID Detection Logic:
Authenticated: Vulnerable OpenSSH versions are detected by running ssh -V command.
Unauthenticated: Vulnerable OpenSSH versions are detected from the banner exposed.

IMPACT:

Successful exploitation allows an attacker to enumerate usernames on a targeted system.

SOLUTION:

Customers are advised to upgrade to OpenSSH 7.8 (https://www.openbsd.org/) or later versions to remediate this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.8 or later (https://www.openbsd.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

Metasploit

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dreambox_openpli_shell
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/gather/credentials/gpp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/ssh/ssh_enumusers
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/plone_popen2
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dlink_dspw215_info_cgi_bof
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/docker_daemon_tcp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/apache_roller_ognl_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/http/ektron_cms400net
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/samba/chain_reply
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/manage/ie_proxypac
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

The Exploit-DB

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration - The Exploit-DB Ref : 45233
Link: http://www.exploit-db.com/exploits/45233

Reference: CVE-2018-15473
Description: OpenSSH < 7.7 - User Enumeration (2) - The Exploit-DB Ref : 45939
Link: http://www.exploit-db.com/exploits/45939

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) - The Exploit-DB Ref : 45210
Link: http://www.exploit-db.com/exploits/45210

Qualys

Reference: CVE-0000-0000
Description: OpenSSH Username Enumeration
Link: http://seclists.org/oss-sec/2018/q3/125

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 OpenSSH Plaintext Recovery Attack Against SSH Vulnerability

QID:	42339
Category:	General remote services
CVE ID:	CVE-2008-5161
Vendor Reference:	openssh-5.2 release note
Bugtraq ID:	32319
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is prone to a plain text recovery attack. The issue is in the SSH protocol specification itself and exists in Secure Shell (SSH) software when used with CBC-mode ciphers.
Affected Versions:
OpenSSH Version 5.1 and earlier.

IMPACT:

This issue can be exploited by a remote unprivileged user to gain access to some of the plain text information from intercepted SSH network traffic, which would otherwise be encrypted.

SOLUTION:

Upgrade to OpenSSH 5.2 or later, available from the OpenSSH OpenSSH Download site (http://www.openssh.com/openbsd.html).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.2: OpenSSH (ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

■■■□□ 3 OpenSSH X11 Forwarding Information Disclosure

QID:	42378
Category:	General remote services
CVE ID:	CVE-2008-3259
Vendor Reference:	OpenSSH 5.1
Bugtraq ID:	30339
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH is exposed to an information disclosure vulnerability caused by an error when binding to previously bound ports that have the SO_REUSEADDR option enabled and the sshd_config X11UseLocalhost option set to no.
Affected Versions:
OpenSSH Versions prior to 5.1 are vulnerable.

IMPACT:

Successfully exploiting this issue may allow an attacker to obtain sensitive information on systems where effective user-id or overlapping bind address checks are not present.

SOLUTION:

Upgrade to OpenSSH 5.1 or later, available from the OpenSSH OpenSSH 5.1 release notes (http://www.openssh.com/txt/release-5.1).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.1 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

■■■□□ 3 OpenSSH Commands Information Disclosure Vulnerability

QID:	42382
Category:	General remote services
CVE ID:	CVE-2012-0814
Vendor Reference:	OpenSSH Forced Command Information Disclosure
Bugtraq ID:	51702
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Openssh-server could allow a remote attacker to obtain sensitive information because of the improper handling of forced commands.

IMPACT:

Only authenticated users can exploit this vulnerability to obtain usernames and other sensitive information.

SOLUTION:

Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site (http://www.openssh.com/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 5.7 (OpenSSH) (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

🟨🟨🟨⬜⬜ 3 OpenSSH J-PAKE Session Key Retrieval Vulnerability

QID:	42384
Category:	General remote services
CVE ID:	CVE-2010-4478
Vendor Reference:	OpenSSH J-PAKE
Bugtraq ID:	45304
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol. This allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.
Affected Software:
OpenSSH versions 5.6 and prior.

IMPACT:

Successful exploitation allows attacker to get access to the remote system.

SOLUTION:

Upgrade to OpenSSH 5.7 or later, available from the OpenSSH Web site (http://www.openssh.com/).
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH J-PAKE (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

🟨🟨🟨⬜⬜ 3 OpenSSH LoginGraceTime Denial of Service Vulnerability

QID:	42413
Category:	General remote services
CVE ID:	CVE-2010-5107
Vendor Reference:	OpenSSH
Bugtraq ID:	58162 , 58162
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
Default OpenSSH installations have an overly long LoginGraceTime and a lack of early connection release for MaxStartups settings. Remote unauthenticated attackers could bypass the LoginGraceTime and MaxStartups thresholds by intermittently transmitting a large number of new TCP connections to the targeted server. This could lead to connection slot exhaustion.

Affected Software:
OpenSSH 6.1 and prior.

IMPACT:

Successful exploitation could allow an unauthenticated remote attacker to cause the targeted server to stop responding to legitimate user queries, leading to a denial of service on the targeted server.

SOLUTION:

Customers are advised to upgrade to OpenSSH 6.2 (http://www.openssh.org/) and apply the associated server configuration settings to remediate this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.2 (http://www.openssh.org/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

QID: 42413 detected on port 22 over TCP - SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1

🟨🟨🟨□□ 3 OpenSSH "X SECURITY" Bypass Vulnerability port 22/tcp

QID:	38611
Category:	General remote services
CVE ID:	CVE-2015-5352
Vendor Reference:	OpenSSH 6.9
Bugtraq ID:	75525
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

A vulnerability has been reported in the application which exist when using ssh -X option, to connect to the SSH client's X server which allow connections without being subject to X11 SECURITY restrictions.
Affected Versions:
OpenSSH prior to version 6.9

IMPACT:

Succesful exploitation of this vulnerability will allow an attacker to interact with X server without being subject to X SECURITY restrictions or authentication

SOLUTION:

Users are advised to upgrade to the latest version of the software available. Refer to OpenSSH 6.9 Release Notes (http://www.openssh.org/txt/release-6.9) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.9 (http://www.openssh.com/)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■■□□ 3 Web Server Stopped Responding port 80/tcp

QID:	86476
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/28/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
The Web server stopped responding to 3 consecutive connection attempts and/or more than 3 consecutive HTTP / HTTPS requests. Consequently, the
service aborted testing for HTTP / HTTPS vulnerabilities. The vulnerabilities already detected are still posted.

IMPACT:
The service was unable to complete testing for HTTP / HTTPS vulnerabilities since the Web server stopped responding.

SOLUTION:
Check the Web server status.
If the Web server was crashed during the scan, please restart the server, report the incident to Customer Support and stop scanning the Web server until the issue is resolved.
If the Web server is unable to process multiple concurrent HTTP / HTTPS requests, please lower the scan harshness level and launch another scan.
If this vulnerability continues to be reported, please contact Customer Support.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
The web server did not respond for 4 consecutive HTTP requests.

■■□□□ 2 OpenSSH Information Disclosure Vulnerability

QID:	38788
Category:	General remote services
CVE ID:	CVE-2011-4327
Vendor Reference:	Openssh
Bugtraq ID:	-
Service Modified:	01/12/2021
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the

SSH protocol.
ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.
Affected Versions:
OpenSSH before 5.8p2
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:
Successful exploitation could disclose sensitive information.

SOLUTION:
Customers are advised to upgrade to OpenSSH 5.8p2 (http://www.openssh.com/txt/portable-keysign-rand-helper.adv) or later to remediate these vulnerabilities.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CVE-2011-4327 (http://www.openssh.com/txt/portable-keysign-rand-helper.adv)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Vulnerable SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

2 OpenSSH "child_set_env()" Security Bypass Issue

QID:	42428
Category:	General remote services
CVE ID:	CVE-2014-2532
Vendor Reference:	OpenSSH 6.6
Bugtraq ID:	66355
Service Modified:	07/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

The security issue is caused by an error within the "child_set_env()" function (usr.bin/ssh/session.c) and can be exploited to bypass intended environment restrictions by using a substring before a wildcard character.
Affected Versions:
OpenSSH Versions prior to 6.6 are affected

IMPACT:
This issue can be exploited by malicious local users to bypass certain security restrictions.

SOLUTION:
Upgrade to OpenSSH 6.6 or later to resolve this issue. Refer to OpenSSH 6.6 Release Notes (http://www.openssh.org/txt/release-6.6) for further information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 6.6: OpenSSH (http://www.openssh.org/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1 detected on port 22 over TCP.

■■□□□ 2 Global User List Found Using Other QIDS

QID:	45002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/16/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
This is the global system user list, which was retrieved during the scan by exploiting one or more vulnerabilities or via authentication provided by user. The Qualys IDs for the vulnerabilities leading to the disclosure of these users are also given in the Result section. Each user will be displayed only once, even though it may be obtained by using different methods.
Note: We did not exploit any vulnerabilities to gather this information in QID 90266, 45027 or 45032.

IMPACT:
These common account(s) can be used by a malicious user to break-in the system via password bruteforcing.

SOLUTION:
To prevent your host from being attacked, do one or more of the following:

Remove (or rename) unnecessary accounts
Shutdown unnecessary network services
Ensure the passwords to these accounts are kept secret
Use a firewall to restrict access to your hosts from unauthorized domains

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	Source Vulnerability (QualysID)
root	38737

Information Gathered (15)

■■■□□ 3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	05/23/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
Service name: SNMP on UDP port 161.
Service name: SSH on TCP port 22.
```

■■□□ 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
EqualLogic Device	TCP/IP Fingerprint	U4444:22

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
172.17.50.102	No registered hostname

1 Firewall Detected

QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	04/21/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
4,6,8,10,12,14,26,28,30,32,34,36,40,225-241,247-250,252-255,266-269,271-279,
283-295,297-308,310,312-317,319-321,326,328-343,352-362,364-368,582-586,
588-591,594-597,599,601-605,621-623,625-626,628-630,632,638-665,675-699,
701-703,708,712-723,725,727-728,732,734,736-739,743,745-746,755-757,766,
768,778-779,784-785,787,789-798,802-820,822-844,846-859,861-868,870-872,
874-885,889-892,894-899,902-910,913-922,924-939,941-949,951-953,956-989,
994,1002-1007,1009,1012-1014,1016-1022,1101-1108,1113,1115-1122,1124-1154,
1156-1166,1168-1169,1171-1206,1208-1211,1213,1215-1219,1223-1224,1226-1233,
1237-1240,1242,1244,1246-1247,1250-1259,1261-1268,1270-1300,1302, and more.
We have omitted from this list 60835 higher ports to keep the report size manageable.
```

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	172.17.1.1	5.70ms	ICMP	
2	172.17.50.102	3.62ms	UDP	80

■□□□□ 1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Scan duration: 2447 seconds

Start time: Sat, Feb 20 2021, 05:37:07 GMT

End time: Sat, Feb 20 2021, 06:17:54 GMT

■□□□□ 1 Scan Activity per Port

QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/24/2020
User Modified:	-
Edited:	No

PCI Vuln:	No

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Protocol	Port	Time
TCP	22	0:05:39
TCP	80	0:40:25
TCP	3002	0:08:12
TCP	9876	0:00:50
TCP	20002	0:01:04
UDP	123	0:01:24
UDP	161	0:03:12

■□□□□ 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting

port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
123	ntp	Network Time Protocol	ntp
161	snmp	SNMP	snmp

■□□□□ 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www-http	World Wide Web HTTP	http	
3002	remoteware-srv	RemoteWare Server	unknown	
3260	unknown	unknown	iSCSI	
9876	sd	Session Director	unknown	
20002	unknown	unknown	unknown	

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 1054	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 20034	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 512	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 25691	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 51100	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 135	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1981	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1434	Port Unreachable

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Average change between subsequent TCP initial sequence numbers is 676523829 with a standard deviation of 541600819. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5110 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

■□□□□ 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 22: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 4 6
Duration: 24 milli seconds

1 Host Name Not Available

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/07/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Attempts to obtain the fully-qualified domain name (FQDN) or the Netbios name failed for this host.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

1 SSH daemon information retrieving port 22/tcp

QID:	38047
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

For Red Hat ES 4:-

SSH1 supported	yes
Supported authentification methods for SSH1	RSA,password
Supported ciphers for SSH1	3des,blowfish
SSH2 supported	yes
Supported keys exchange algorithm for SSH2	diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc, rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc, rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96, hmac-md5-96
Supported encryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96, hmac-md5-96
Supported authentification methods for SSH2	publickey,gssapi-with-mic,password

IMPACT:
Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with

arbitrary data.

SOLUTION:
SSH version 2 is preferred over SSH version 1.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
Supported host key algorithms for SSH2	ssh-rsa
Supported decryption ciphers for SSH2	aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
Supported encryption ciphers for SSH2	aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
Supported decryption macs for SSH2	hmac-sha1, hmac-sha1-96
Supported encryption macs for SSH2	hmac-sha1, hmac-sha1-96
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, password

■□□□□ 1 SSH Banner port 22/tcp

QID:	38050
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/30/2020
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.
QID Detection Logic:
The QID checks for SSH in the banner of the response.

IMPACT:
NA

SOLUTION:
NA

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

```
SSH-2.0-OpenSSH_5.0 NetBSD_Secure_Shell-20080403+-hpn13v1
```

Appendix

Hosts Scanned (IP)

172.16.1.1, 172.16.1.12-172.16.1.14, 172.16.1.80, 172.16.1.253-172.16.1.254, 172.16.10.5, 172.16.10.22, 172.16.30.15, 172.16.30.20-172.16.30.22, 172.16.50.90, 172.16.50.100-172.16.50.102, 172.17.1.1, 172.17.1.15-172.17.1.17, 172.17.1.80, 172.17.1.253-172.17.1.254, 172.17.10.5, 172.17.10.20-172.17.10.21, 172.17.20.20-172.17.20.23, 172.17.30.15, 172.17.50.100-172.17.50.102

Target distribution across scanner appliances

ACOSTA : 172.16.1.1, 172.16.1.12-172.16.1.14, 172.16.1.80, 172.16.1.253-172.16.1.254, 172.16.10.5, 172.16.10.22, 172.16.30.15, 172.16.30.20-172.16.30.22, 172.16.50.90, 172.16.50.100-172.16.50.102, 172.17.1.1, 172.17.1.15-172.17.1.17, 172.17.1.80, 172.17.1.253-172.17.1.254, 172.17.10.5, 172.17.10.20-172.17.10.22, 172.17.20.20-172.17.20.23, 172.17.30.15, 172.17.30.20-172.17.30.22, 172.17.50.100-172.17.50.102

Hosts Not Scanned

Hosts Not Alive (IP) (4)

172.17.10.22, 172.17.30.20-172.17.30.22

Options Profile

Combined Profiles

Scan Settings

Ports:	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Close Vulnerabilities on Dead Hosts Count:	Off
Purge old host data when OS changes:	Off
Load Balancer Detection:	On
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Intrusive Checks:	Excluded
Password Brute Forcing:	
System:	Standard
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled

InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Kubernetes:	Disabled
SAP IQ:	Disabled
Overall Performance:	Normal
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30
Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	On
Ignore all TCP RST packets:	On
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
🟥⬜⬜⬜ 1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
🟥🟥⬜⬜ 2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
🟥🟥🟥⬜ 3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
🟥🟥🟥🟥 4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.

Severity	Level	Description
🟥🟥🟥🟥🟥 5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
🟨□□□□ 1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
🟨🟨□□□ 2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
🟨🟨🟨□□ 3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
🟨🟨🟨🟨□ 4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
🟨🟨🟨🟨🟨 5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
🟦□□□□ 1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
🟦🟦□□□ 2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
🟦🟦🟦□□ 3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free.