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 23:12:25 (GMT-0500)
Client:	Elevate Consult
Launch Date:	02/20/2021 at 01:35:16 (GMT-0500)
Active Hosts:	15
Total Hosts:	32
Type:	Scheduled
Status:	Finished
Reference:	scan/1613802916.15376
External Scanners:	64.39.108.61 (Scanner 12.2.62-1, Vulnerability Signatures 2.5.112-3)
Duration:	00:32:11
Title:	Acosta External DR and QA
Asset Groups:	Acosta External DR & QA, Acosta External Production
IPs:	64.135.81.16-64.135.81.31, 173.230.231.240-173.230.231.255
Excluded IPs:	-
Options Profile:	Initial Options

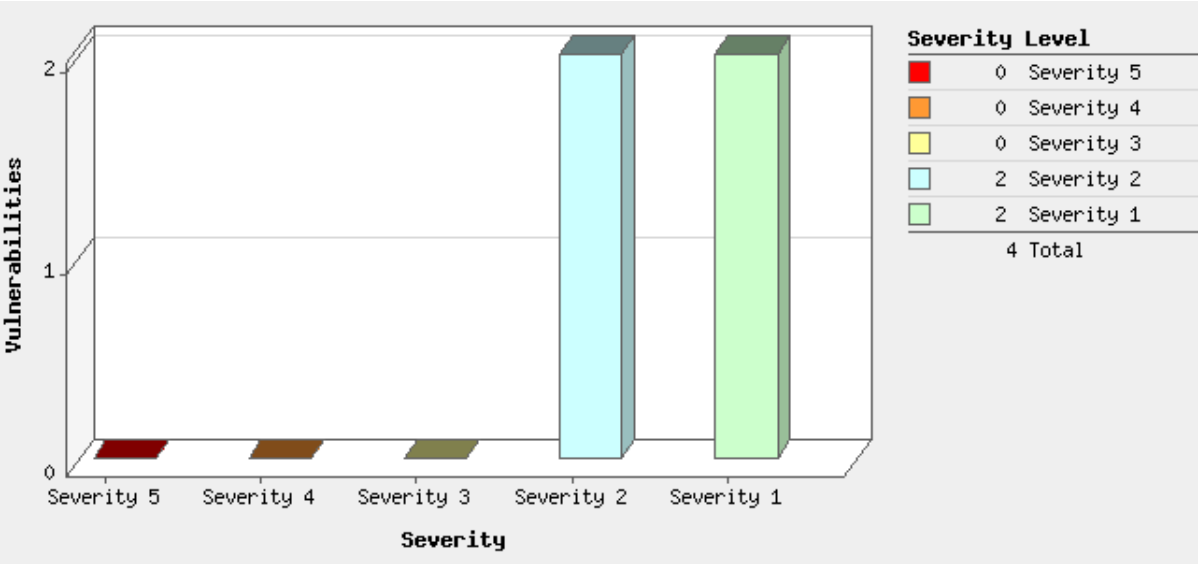
Summary of Vulnerabilities

Vulnerabilities Total	393	Security Risk (Avg)	0.6

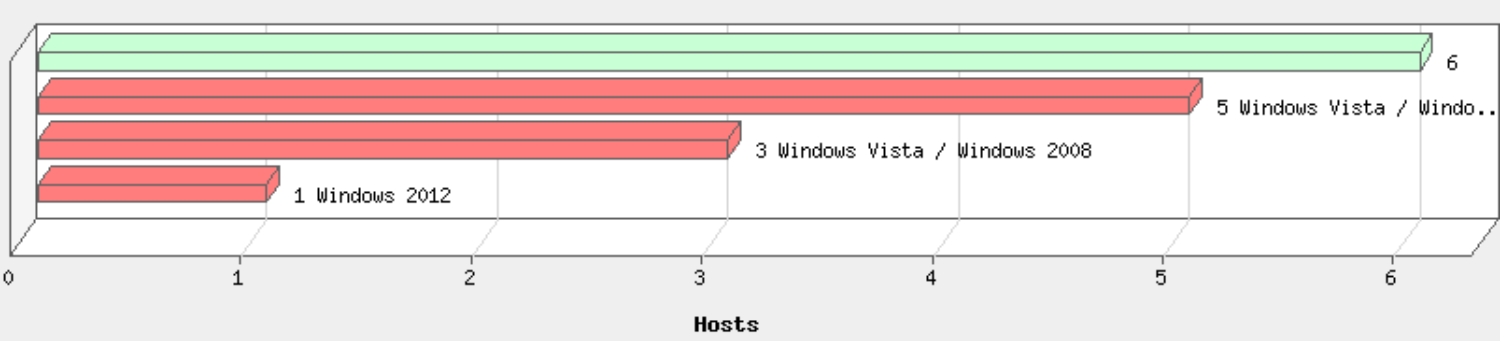
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	2	9	11
2	2	0	42	44
1	2	1	335	338
Total	4	3	386	393

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	156	156
General remote services	3	3	73	79
TCP/IP	1	0	61	62
Web server	0	0	45	45
CGI	0	0	37	37
Total	4	3	372	379

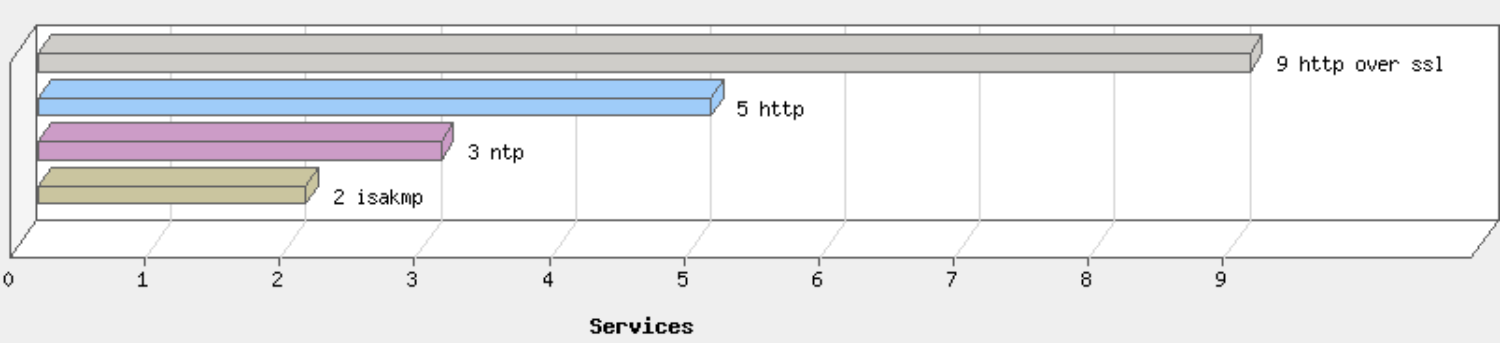
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

64.135.81.16 (-, -)

Information Gathered (9)

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
64.135.81.16	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.
55,78,81-83,86-87,112,116-117,157,159,182,190-192,202,205-206,208,220,
256,348,363,384,412,414,421,453,464,472,477,500,507,516,529,545,549,565,
576,578-579,615,634,636-637,700,771,773,911,1000,1024,1035,1051,1063,
1072,1078,1083,1096-1097,1220,1363,1367,1375,1378,1386,1430,1434,1452,
1475,1491,1509,1517,1533,1576,1578,1589,1608,1616,1640,1658,1676,1681,
1697,1713,1736,1740,1742,1744,1750,1756,1768,1780,1811,1903,1906-1907,
1988-1989,1998-1999,2009,2015,2038,2100,2120,2161,2202,2232,2279-2280,
2381,2532,2700,2788,3000,3007,3143,3351,3457,4100,4333,4443,4448,4672,
4903,5021,5031,5150,5303,5400-5401,5599-5600,5742,6018,6027,6052,6142,
6145,6389, and more.
We have omitted from this list 31 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

The network handle is: HOST-BROADBANDONE
Network description:
BroadbandONE, LLC

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The ISP network handle is: NET-65-158-181-0-1
ISP Network description:
Qwest Communications Company, LLC TAMP01-WAN-65-158-181-0

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	64.39.111.3	0.36ms	ICMP	
2	216.35.14.45	0.80ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.78ms	ICMP	
5	67.14.29.166	74.61ms	ICMP	
6	65.158.181.250	74.79ms	ICMP	
7	64.135.81.16	78.67ms	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: 520 seconds

Start time: Sat, Feb 20 2021, 06:37:34 GMT

End time: Sat, Feb 20 2021, 06:46:14 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	0:01:24

 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

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

64.135.81.17 (-, -)

Information Gathered (10)

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
64.135.81.17	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.
68,167,396

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: HOST-BROADBANDONE
Network description:
BroadbandONE, LLC

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

The ISP network handle is: NET-65-158-181-0-1
ISP Network description:
Qwest Communications Company, LLC TAMP01-WAN-65-158-181-0

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	64.39.111.3	0.39ms	ICMP	
2	216.35.14.45	0.36ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.77ms	ICMP	
5	67.14.29.166	74.64ms	ICMP	
6	65.158.181.250	74.78ms	ICMP	
7	64.135.81.17	77.35ms	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: 585 seconds

Start time: Sat, Feb 20 2021, 06:37:33 GMT

End time: Sat, Feb 20 2021, 06:47:18 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
UDP	123	0:01:24

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

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 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

64.135.81.18 (-, -)

Vulnerabilities (1)

2 Pre-shared Key Off-line Bruteforcing Using IKE Aggressive Mode port 500/udp

QID:	38498
Category:	General remote services
CVE ID:	CVE-2002-1623
Vendor Reference:	cisco-sn-20030422-ike
Bugtraq ID:	7423, 5607
Service Modified:	08/14/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

IKE is used during Phase 1 and Phase 2 of establishing an IPSec connection. Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. Every participant in IKE must possess a key which may be either pre-shared (PSK) or a public key. There are inherent risks to configurations that use pre-shared keys which are exaggerated when Aggressive Mode is used.
QID Detection Logic
This QID checks if the peer accepts the proposal which specifies "Pre-shared key" as authentication method in aggressive mode,enabled with pre-shared keys during IKE phase 1 negotiation and returns the hash of ISAKMP response.

IMPACT:

Using Aggressive Mode with pre-shared keys is the least secure option. In this particular scenario, it is possible for an attacker to gather all necessary information in order to mount an off-line dictionary (brute force) attack on the pre-shared keys. For more information about this type of attack, visit http://www.ernw.de/download/pskattack.pdf (http://www.ernw.de/download/pskattack.pdf).

SOLUTION:

IKE Aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

isakmp hash(key + identity): 494da69a229de8b5f28abbef17cc51c640d4d4eb

Potential Vulnerabilities (1)

3 Weak IPsec Encryption Settings port 500/udp

QID:	38115
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/06/2017
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

This host contains an ISAKMP/IKE key exchange server to negotiate encryption keys for IPsec Virtual Private Networks (VPNs). The configuration of the server allows clients to establish VPN connections with insecure encryption settings or key lengths. Once established, these connections may allow remote malicious users with access to the VPN data stream to recover the session key used in the connection by performing brute-force key space searches.
Note:
This QID will be reported as a Potential Vulnerability (not as a Vulnerability) on some versions of IOS because an ISAKMP SA with weak settings can be established first, and then rejected later by a policy check. Without having VPN authentication credentials, it is impossible to differentiate between this type of setup and a setup that truly allows ISAKMP SA with weak settings.

IMPACT:
A malicious user with access to the VPN data stream may be able to recover the session key of a VPN connection. This would then provide access to all data sent across the VPN connection, which may include passwords and sensitive files.

SOLUTION:
Disable the encryption algorithm "DES" (key length of 56 bits) and the key exchange algorithm DH768 (MODP768). Secure replacements are 3DES and DH2048.
MSFT has further details under Microsoft Guidance : What is IPSEC? (https://technet.microsoft.com/library/cc776369.aspx).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

Algorithm	Description
DES	Data Encryption Standard (56 bits)

Information Gathered (14)

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: ISAKMP on UDP port 500.

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
64.135.81.18	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: 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.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-381,383-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1559,1561-1625,1636-1705,
1707-1721,1723-1774,1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,
1973,1981,1985-1999,2001-2028,2030,2032-2033,2035,2038,2040-2049,2053,
2065, and more.
We have omitted from this list 703 higher ports to keep the report size manageable.

 1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

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

RESULTS:

The network handle is: HOST-BROADBANDONE
Network description:
BroadbandONE, LLC

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

The ISP network handle is: NET-65-158-181-0-1
ISP Network description:
Qwest Communications Company, LLC TAMP01-WAN-65-158-181-0

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	64.39.111.3	0.43ms	ICMP	
2	216.35.14.45	0.51ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.83ms	ICMP	
5	67.14.29.166	74.67ms	ICMP	
6	65.158.181.250	75.18ms	ICMP	
7	66.216.2.160	76.83ms	ICMP	
8	64.135.81.18	76.55ms	ICMP	

1 Virtual Private Networks

QID:	45013
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/01/1999
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This host allows Virtual Private Network connections to be established from remote VPN clients.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

Port	Service	Description
500	ISAKMP/IKE	ISAKMP/IKE key exchange for IPsec Virtual Private Network

1 VPN Authentications

QID:	45014
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-

Bugtraq ID:	-
Service Modified:	11/10/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following authentication policies are supported by the VPN servers on 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:

Authentication	Description
Preshared Key	Client and server share a secret, preconfigured key.

1 IKE Service Implementation Identified

QID:	45018
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/23/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The IKE service implementation active on this host can be identified from a remote system using IKE fingerprinting. All IKE service implementations have subtle differences that can be seen in their responses to specially crafted packets. According to the results of this "fingerprinting" technique, the IKE service implementation is among those listed below.
If one or more of these subtle differences is modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the IKE implementation may not be detected correctly.

IMPACT:
Through acquired knowledge of the IKE implementation, an attacker can launch further attacks against the service or try to bypass it.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
Cisco PIX Firewall/VPN Concentrator

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: 742 seconds

Start time: Sat, Feb 20 2021, 06:37:33 GMT

End time: Sat, Feb 20 2021, 06:49:55 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	500	0:04:51

 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
500	isakmp	isakmp	isakmp

 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 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

64.135.81.19 (rdg.enterate.com, -) Windows Vista / Windows 2008 / Windows 7 / Windows 2012

Information Gathered (29)

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 Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:443

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, 14 hours, and 45 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

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

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
64.135.81.19	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, 80, 111, 135, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100,
2102, and more.
We have omitted from this list 704 higher ports to keep the report size manageable.

 1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

The network handle is: HOST-BROADBANDONE
Network description:
BroadbandONE, LLC

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The ISP network handle is: NET-65-158-181-0-1
ISP Network description:
Qwest Communications Company, LLC TAMP01-WAN-65-158-181-0

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	64.39.111.3	0.41ms	ICMP	
2	216.35.14.45	0.35ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.76ms	ICMP	
5	67.14.29.166	74.60ms	ICMP	
6	65.158.181.250	74.89ms	ICMP	
7	66.216.2.160	76.95ms	ICMP	
8	64.135.81.19	77.23ms	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: 1413 seconds

Start time: Sat, Feb 20 2021, 06:37:34 GMT

End time: Sat, Feb 20 2021, 07:01:07 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
rdg.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	443	1:35:55

 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
443	https	http protocol over TLS/SSL	http 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 1000519842 with a standard deviation of 586214243. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4995 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 443: 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 1 1 1
Duration: 37 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: 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 06:42:01 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 06:44:30 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:64.135.81.19:443

GET /Q_Evasive/ HTTP/1.1
Host:64.135.81.19:443

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 06:45:59 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>
<h1>Server Error</h1>

<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>

</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 06:45:59 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>
<h1>Server Error</h1>

<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>

</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: 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 06:42:01 GMT
Connection: keep-alive
Content-Length: 1208

 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

64.135.81.20 (qa-web1.enterate.com, -) Windows 2012

Information Gathered (37)

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

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	TCP/IP Fingerprint	U3423:80

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 31 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

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

 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
64.135.81.20	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, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-79,81-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100, and more.
We have omitted from this list 705 higher ports to keep the report size manageable.

 1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The network handle is: HOST-BROADBANDONE
Network description:
BroadbandONE, LLC

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The ISP network handle is: NET-65-158-181-0-1
ISP Network description:
Qwest Communications Company, LLC TAMP01-WAN-65-158-181-0

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	64.39.111.3	0.40ms	ICMP	
2	216.35.14.45	0.37ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.73ms	ICMP	
5	67.14.29.166	74.68ms	ICMP	
6	65.158.181.250	75.08ms	ICMP	
7	66.216.2.160	76.56ms	ICMP	
8	64.135.81.20	76.69ms	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: 1866 seconds

Start time: Sat, Feb 20 2021, 06:37:33 GMT

End time: Sat, Feb 20 2021, 07:08:39 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	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	80	1:11:59
TCP	443	2:02:53

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	
443	https	http protocol over TLS/SSL	http 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 1273078580 with a standard deviation of 426100401. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5387 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 2 2 2 2
Duration: 30 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</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 06:40:19 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 06:47:49 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 06:51:55 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:64.135.81.20:443

GET /Q_Evasive/ HTTP/1.1
Host:64.135.81.20:443

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 06:47:27 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 06:47:27 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 06:47:49 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

64.135.81.21 (qa-app1.enterate.com, -) Windows Vista / Windows 2008 / Windows 7 / Windows 2012

Information Gathered (35)

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 Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:443

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 42 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

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

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
64.135.81.21	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:
Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100,
2102, and more.
We have omitted from this list 702 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The network handle is: HOST-BROADBANDONE
Network description:
BroadbandONE, LLC

 1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

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

RESULTS:

The ISP network handle is: NET-65-158-181-0-1
ISP Network description:
Qwest Communications Company, LLC TAMP01-WAN-65-158-181-0

 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	64.39.111.3	0.40ms	ICMP	
2	216.35.14.45	0.37ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.76ms	ICMP	
5	67.14.29.166	74.64ms	ICMP	
6	65.158.181.250	74.66ms	ICMP	
7	66.216.2.160	77.15ms	ICMP	
8	64.135.81.21	77.08ms	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: 1606 seconds

Start time: Sat, Feb 20 2021, 06:37:33 GMT

End time: Sat, Feb 20 2021, 07:04:19 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	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	443	1:49:58
TCP	8080	0:19:06
TCP	8181	0:15:53

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
443	https	http protocol over TLS/SSL	http over ssl	
8080	http-alt	HTTP Alternate (see port 80)	unknown	
8181	IpSwitch-IMail-WebStatus	IpSwitch-IMail-WebStatus	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

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 980261863 with a standard deviation of 636010443. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5299 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 443: 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 2
Duration: 32 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 06:44:01 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 06:46:57 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/	22454507595524569 63fa12ff1f76d86e0232663adc04b7f5dc6835c6ee20f02	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-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 06:44:01 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

64.135.81.24 (qa-app2.enterate.com, -) Windows Vista / Windows 2008 / Windows 7 / Windows 2012

Vulnerabilities (1)

1 SSL/TLS Server supports TLSv1.1 port 443/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

Information Gathered (51)

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-app2.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 Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:443

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, 22 hours, and 3 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

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

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
64.135.81.24	qa-app2.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, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,

600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100,
2102, and more.
We have omitted from this list 702 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The network handle is: HOST-BROADBANDONE
Network description:
BroadbandONE, LLC

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The ISP network handle is: NET-65-158-181-0-1
ISP Network description:
Qwest Communications Company, LLC TAMP01-WAN-65-158-181-0

 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	64.39.111.3	0.40ms	ICMP	
2	216.35.14.45	0.36ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.72ms	ICMP	
5	67.14.29.166	74.59ms	ICMP	
6	65.158.181.250	74.84ms	ICMP	
7	66.216.2.160	76.48ms	ICMP	
8	64.135.81.24	76.65ms	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: 1496 seconds

Start time: Sat, Feb 20 2021, 06:37:34 GMT

End time: Sat, Feb 20 2021, 07:02:30 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
qa-app2.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	443	1:33:25
TCP	8080	0:02:35
TCP	8181	0:06:04

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
443	https	http protocol over TLS/SSL	http over ssl	
8080	http-alt	HTTP Alternate (see port 80)	http	
8181	IpSwitch-IMail-WebStatus	IpSwitch-IMail-WebStatus	http 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 1251116928 with a standard deviation of 608274658. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4995 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 443: 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
Duration: 31 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-app2.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 06:43:35 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-app2.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 06:45:37 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>
```

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 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:

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

1 SSL/TLS invalid protocol version tolerance

port 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	rejected
0399	rejected
0400	rejected
0499	rejected

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
TLSv1.1					
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 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
TLSv1.1	
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 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-app2.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 06:39:29 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&amp;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-app2.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 06:39:29 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">
 <table width="100%" border="0" cellspacing="0" cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> oracle.com </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993"> GlassFish Server </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
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.
To manage a server on the local host with the default administration port, go to the Administration Console.
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>

For production deployments, consider Oracle GlassFish Server with Oracle Premier Support for Software. 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.
<h2>Install and update additional software components</h2>
Use the Update Tool to install and update additional technologies and frameworks such as:

OSGi HTTP Service
Generic Resource Adapter for JMS
OSGi Administration Console

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:

Enterprise Java Beans
Metro
Jersey

To improve the user experience and optimize offerings to users, Oracle collects data about GlassFish Server usage that is transmitted by the Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by this process.
-->
<h2>Join the GlassFish community</h2>
Visit the GlassFish Community 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™ Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.
<h2>Learn more about GlassFish Server</h2>
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.
<hr style="width: 80%; height: 2px;">
Company Info | Contact |
Copyright © 2010, 2014 Oracle Corporation | Legal Notices </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

1 Web Server Supports HTTP Request Pipelining port 8080/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:64.135.81.24:8080

GET /Q_Evasive/ HTTP/1.1
Host:64.135.81.24:8080

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 06:46:58 GMT
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">
 <table width="100%" border="0" cellspacing="0" cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> oracle.com </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993"> GlassFish Server </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
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.
To manage a server on the local host with the default administration port, go to the Administration Console.
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
For production deployments, consider Oracle GlassFish Server with Oracle Premier Support for Software. 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.
<h2>Install and update additional software components</h2>
Use the Update Tool to install and update additional technologies and frameworks such as:

OSGi HTTP Service
Generic Resource Adapter for JMS
OSGi Administration Console

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:

Enterprise Java Beans
Metro
Jersey

To improve the user experience and optimize offerings to users, Oracle collects data about GlassFish Server usage that is transmitted by the Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by this process.
-->
<h2>Join the GlassFish community</h2>
Visit the GlassFish Community 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™ Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.
<h2>Learn more about GlassFish Server</h2>
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.
<hr style="width: 80%; height: 2px;">
Company Info | Contact |
Copyright © 2010, 2014 Oracle Corporation | Legal Notices </body></html>
HTTP/1.1 404 Not Found
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)
Content-Language:
Content-Type: text/html
Date: Sat, 20 Feb 2021 06:46:58 GMT
Content-Length: 1082

<!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><title>GlassFish Server Open Source Edition 4.1 - Error report</title><style type="text/css"><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,

Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}HR {color : #525D76;}--></style> </head><body><h1>HTTP Status 404 - Not Found</h1><hr/> type Status report messageNot Found descriptionThe requested resource is not available. <hr/><h3>GlassFish Server Open Source Edition 4.1 </h3></body></html>

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 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-app2.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 06:43:35 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 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-app2.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 06:47:13 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>
```

Metro
Jersey

To improve the user experience and optimize offerings to users, Oracle collects data about GlassFish Server usage that is transmitted by the Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by this process.
-->
<h2>Join the GlassFish community</h2>
Visit the GlassFish Community 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™ Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.
<h2>Learn more about GlassFish Server</h2>
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.
<hr style="width: 80%; height: 2px;">
Company Info | Contact |
Copyright © 2010, 2014 Oracle Corporation | Legal Notices </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-app2.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 06:47:13 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.

-->
<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">
 <table width="100%" border="0" cellspacing="0" cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> oracle.com </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993"> GlassFish Server </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
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.
To manage a server on the local host with the default administration port, go to the Administration Console.
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
For production deployments, consider Oracle GlassFish Server with Oracle Premier Support for Software. 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.
<h2>Install and update additional software components</h2>
Use the Update Tool to install and update additional technologies and frameworks such as:

OSGi HTTP Service
Generic Resource Adapter for JMS
OSGi Administration Console

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:

Enterprise Java Beans
Metro
Jersey

To improve the user experience and optimize offerings to users, Oracle collects data about GlassFish Server usage that is transmitted by the Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by this process.
-->
<h2>Join the GlassFish community</h2>
Visit the GlassFish Community 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™ Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.
<h2>Learn more about GlassFish Server</h2>
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.
<hr style="width: 80%; height: 2px;">
Company Info | Contact |
</body></html>

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 Web Server Supports HTTP Request Pipelining port 8181/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:64.135.81.24:8181

GET /Q_Evasive/ HTTP/1.1
Host:64.135.81.24:8181

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 06:47:10 GMT
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">
 <table width="100%" border="0" cellspacing="0" cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> oracle.com </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993"> GlassFish Server </td></tr>
</tbody>
</table>
<h1>Your server is now running</h1>
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.
To manage a server on the local host with the default administration port, go to the Administration Console.
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
For production deployments, consider Oracle GlassFish Server with Oracle Premier Support for Software. 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.
<h2>Install and update additional software components</h2>
Use the Update Tool to install and update additional technologies and

frameworks such as:

OSGi HTTP Service
Generic Resource Adapter for JMS
OSGi Administration Console

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:

Enterprise Java Beans
Metro
Jersey

To improve the user experience and optimize offerings to users, Oracle collects data about GlassFish Server usage that is transmitted by the Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by this process.
-->
<h2>Join the GlassFish community</h2>
Visit the GlassFish Community 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™ Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.
<h2>Learn more about GlassFish Server</h2>
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.
<hr style="width: 80%; height: 2px;">
Company Info | Contact |
Copyright © 2010, 2014 Oracle Corporation | Legal Notices </body></html>
HTTP/1.1 404 Not Found
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)
Content-Language:
Content-Type: text/html
Date: Sat, 20 Feb 2021 06:47:10 GMT
Content-Length: 1082

<!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><title>GlassFish Server Open Source Edition 4.1 - Error report</title><style type="text/css"><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}HR {color : #525D76;}--></style> </head><body><h1>HTTP Status 404 - Not Found</h1><hr/> type Status report messageNot Found descriptionThe requested resource is not available. <hr/><h3>GlassFish Server Open Source Edition 4.1 </h3></body></html>

64.135.81.26 (qa-web2.enterate.com, -) Windows Vista / Windows 2008

Information Gathered (39)

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 Vista / Windows 2008	TCP/IP Fingerprint	U3423:80

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, 20 hours, and 29 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

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

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
64.135.81.26	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, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-79,81-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100, and more.
We have omitted from this list 705 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The network handle is: HOST-BROADBANDONE
Network description:
BroadbandONE, LLC

1 Internet Service Provider

QID:	45005
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The ISP network handle is: NET-65-158-181-0-1
ISP Network description:
Qwest Communications Company, LLC TAMP01-WAN-65-158-181-0

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	64.39.111.3	0.37ms	ICMP	
2	216.35.14.45	0.35ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.73ms	ICMP	
5	67.14.29.166	74.66ms	ICMP	
6	65.158.181.250	74.76ms	ICMP	
7	66.216.2.160	76.47ms	ICMP	
8	64.135.81.26	76.71ms	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: 1764 seconds

Start time: Sat, Feb 20 2021, 06:37:34 GMT

End time: Sat, Feb 20 2021, 07:06:58 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	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	80	1:08:32
TCP	443	1:33:05

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	
443	https	http protocol over TLS/SSL	http 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 883662323 with a standard deviation of 636513583. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4993 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 2
Duration: 31 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-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 06:47:15 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 06:49:41 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 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</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 06:39:56 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 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 06:47:15 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

64.135.81.31 (-, -)

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
64.135.81.31	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: 598 seconds

Start time: Sat, Feb 20 2021, 06:37:33 GMT

End time: Sat, Feb 20 2021, 06:47:31 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	0:01:24

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


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

173.230.231.241 (-, -)

Vulnerabilities (1)

1 ICMP Timestamp Request

QID:	82003
Category:	TCP/IP
CVE ID:	CVE-1999-0524
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/28/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.
However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.
It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
Timestamp of host (network byte ordering): 06:37:13 GMT

Information Gathered (10)

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
173.230.231.241	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, 23.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
22-23,123,161

1 Target Network Information

QID:	45004

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The network handle is: WEBHOSTING-NET
Network description:
Webhosting.Net, Inc.

 1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

The ISP network handle is: PNAP-12-2002
ISP Network description:
Internap Holding LLC

 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	64.39.111.3	0.37ms	ICMP	
2	216.35.14.45	0.42ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.76ms	ICMP	
5	67.14.34.38	4.33ms	ICMP	
6	4.68.62.77	7.42ms	ICMP	
7	80.239.195.62	5.66ms	ICMP	
8	62.115.125.160	5.65ms	ICMP	
9	62.115.116.41	11.86ms	ICMP	
10	62.115.123.136	43.75ms	ICMP	
11	80.91.246.74	59.83ms	ICMP	
12	62.115.113.49	74.81ms	ICMP	
13	62.115.125.7	75.12ms	ICMP	
14	62.115.12.170	76.29ms	ICMP	
15	69.25.0.10	74.67ms	ICMP	
16	69.25.5.182	75.20ms	ICMP	
17	173.230.231.241	78.30ms	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: 307 seconds

Start time: Sat, Feb 20 2021, 06:37:10 GMT

End time: Sat, Feb 20 2021, 06:42:17 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	161	0:00:56
UDP	514	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

161	snmp	SNMP	unknown
514	syslog	syslog	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 80	Port Unreachable
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 6771	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 58493	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7308	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7306	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1039	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 4590	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 17	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1028	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1031	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	06:37:13 GMT

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

173.230.231.242 (-, -)

Vulnerabilities (1)

2 Pre-shared Key Off-line Bruteforcing Using IKE Aggressive Mode port 500/udp

QID:	38498
Category:	General remote services
CVE ID:	CVE-2002-1623
Vendor Reference:	cisco-sn-20030422-ike
Bugtraq ID:	7423, 5607
Service Modified:	08/14/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
IKE is used during Phase 1 and Phase 2 of establishing an IPSec connection. Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. Every participant in IKE must possess a key which may be either pre-shared (PSK) or a public key. There are inherent risks to configurations that use pre-shared keys which are exaggerated when Aggressive Mode is used.
QID Detection Logic
This QID checks if the peer accepts the proposal which specifies "Pre-shared key" as authentication method in aggressive mode,enabled with pre-shared keys during IKE phase 1 negotiation and returns the hash of ISAKMP response.

IMPACT:
Using Aggressive Mode with pre-shared keys is the least secure option. In this particular scenario, it is possible for an attacker to gather all necessary information in order to mount an off-line dictionary (brute force) attack on the pre-shared keys. For more information about this type of attack, visit http://www.ernw.de/download/pskattack.pdf (http://www.ernw.de/download/pskattack.pdf).

SOLUTION:
IKE Aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
isakmp hash(key + identity): 77548f523e3337db6bf945913ae3f7276b269e45

Potential Vulnerabilities (1)

3 Weak IPsec Encryption Settings port 500/udp

QID:	38115
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/06/2017
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
This host contains an ISAKMP/IKE key exchange server to negotiate encryption keys for IPsec Virtual Private Networks (VPNs). The configuration of the server allows clients to establish VPN connections with insecure encryption settings or key lengths. Once established, these connections may allow remote malicious users with access to the VPN data stream to recover the session key used in the connection by performing brute-force key space searches.
Note:
This QID will be reported as a Potential Vulnerability (not as a Vulnerability) on some versions of IOS because an ISAKMP SA with weak settings can be established first, and then rejected later by a policy check. Without having VPN authentication credentials, it is impossible to differentiate between this type of setup and a setup that truly allows ISAKMP SA with weak
settings.

IMPACT:
A malicious user with access to the VPN data stream may be able to recover the session key of a VPN connection. This would then provide access to all data sent across the VPN connection, which may include passwords and sensitive files.

SOLUTION:
Disable the encryption algorithm "DES" (key length of 56 bits) and the key exchange algorithm DH768 (MODP768). Secure replacements are 3DES and DH2048.
MSFT has further details under Microsoft Guidance : What is IPSEC? (https://technet.microsoft.com/library/cc776369.aspx).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

Algorithm	Description
DES	Data Encryption Standard (56 bits)

Information Gathered (14)

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: ISAKMP on UDP port 500.

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
173.230.231.242	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: 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.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-381,383-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1559,1561-1625,1636-1705,
1707-1721,1723-1774,1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,
1973,1981,1985-1999,2001-2028,2030,2032-2033,2035,2038,2040-2049,2053,
2065, and more.
We have omitted from this list 703 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

The network handle is: WEBHOSTING-NET
Network description:
Webhosting.Net, Inc.

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

The ISP network handle is: NET-216-52-163-128-1
ISP Network description:
webhosting.net INAP-MIA003-WEBHOSTING-54358

 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	64.39.111.3	0.36ms	ICMP	
2	216.35.14.45	0.38ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.78ms	ICMP	
5	67.14.34.38	4.43ms	ICMP	
6	4.68.62.77	4.85ms	ICMP	
7	80.239.195.62	5.37ms	ICMP	
8	62.115.125.160	5.69ms	ICMP	
9	62.115.116.41	12.00ms	ICMP	
10	62.115.123.136	43.68ms	ICMP	
11	62.115.123.201	59.81ms	ICMP	
12	62.115.113.49	75.08ms	ICMP	
13	62.115.125.7	74.65ms	ICMP	
14	62.115.12.170	75.26ms	ICMP	
15	69.25.0.10	74.50ms	ICMP	
16	69.25.5.182	75.18ms	ICMP	
17	216.52.163.130	78.16ms	ICMP	
18	173.230.231.242	74.86ms	ICMP	

1 Virtual Private Networks

QID:	45013
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/01/1999
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This host allows Virtual Private Network connections to be established from remote VPN clients.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

Port	Service	Description
500	ISAKMP/IKE	ISAKMP/IKE key exchange for IPsec Virtual Private Network

1 VPN Authentications

QID:	45014
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/10/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following authentication policies are supported by the VPN servers on 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:

Authentication	Description
Preshared Key	Client and server share a secret, preconfigured key.

1 IKE Service Implementation Identified

QID:	45018
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/23/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The IKE service implementation active on this host can be identified from a remote system using IKE fingerprinting. All IKE service implementations have subtle differences that can be seen in their responses to specially crafted packets. According to the results of this "fingerprinting" technique, the IKE service implementation is among those listed below.
If one or more of these subtle differences is modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the IKE implementation may not be detected correctly.

IMPACT:
Through acquired knowledge of the IKE implementation, an attacker can launch further attacks against the service or try to bypass it.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
Cisco PIX Firewall/VPN Concentrator

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: 740 seconds

Start time: Sat, Feb 20 2021, 06:37:33 GMT

End time: Sat, Feb 20 2021, 06:49:53 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	500	0:04:49

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
500	isakmp	isakmp	isakmp

 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 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

173.230.231.243 (rdg.enterate.com, -) Windows Vista / Windows 2008 / Windows 7 / Windows 2012

Information Gathered (34)

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: 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 Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:443

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 22 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

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

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
173.230.231.243	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, 80, 111, 135, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100,
2102, and more.
We have omitted from this list 704 higher ports to keep the report size manageable.

 1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:

This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

The network handle is: WEBHOSTING-NET
Network description:
Webhosting.Net, Inc.

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:

The ISP network handle is: NET-216-52-163-128-1
ISP Network description:
webhosting.net INAP-MIA003-WEBHOSTING-54358

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	64.39.111.3	0.40ms	ICMP	
2	216.35.14.45	0.42ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.74ms	ICMP	
5	67.14.34.38	4.42ms	ICMP	
6	4.68.62.77	5.49ms	ICMP	
7	80.239.195.62	5.81ms	ICMP	
8	62.115.125.160	5.70ms	UDP	80
9	62.115.116.41	12.09ms	ICMP	
10	62.115.123.136	43.83ms	ICMP	
11	80.91.246.74	59.86ms	ICMP	
12	62.115.113.49	74.92ms	ICMP	
13	62.115.125.7	75.29ms	ICMP	
14	62.115.12.170	75.34ms	ICMP	
15	69.25.0.10	74.67ms	ICMP	
16	69.25.5.182	75.12ms	ICMP	
17	216.52.163.130	77.36ms	ICMP	
18	173.230.231.243	75.65ms	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: 1483 seconds

Start time: Sat, Feb 20 2021, 06:37:33 GMT

End time: Sat, Feb 20 2021, 07:02:16 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
rdg.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	443	1:29:11

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
443	https	http protocol over TLS/SSL	http 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 1050731421 with a standard deviation of 630677536. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4998 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 443: 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: 32 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: 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 06:43:45 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 (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 06:45:48 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=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

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: 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 06:43:45 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 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
/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: 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 06:43:45 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>
```

173.230.231.244 (web1.enterate.com, -) Windows Vista / Windows 2008

Information Gathered (45)

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

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 Vista / Windows 2008	TCP/IP Fingerprint	U3423:80

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, 23 hours, and 40 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

 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

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
173.230.231.244	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, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-79,81-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100, and more.
We have omitted from this list 705 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The network handle is: WEBHOSTING-NET
Network description:
Webhosting.Net, Inc.

1 Internet Service Provider

QID:	45005
Category:	Information gathering

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The ISP network handle is: NET-216-52-163-128-1
ISP Network description:
webhosting.net INAP-MIA003-WEBHOSTING-54358

 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	64.39.111.3	0.34ms	ICMP	
2	216.35.14.45	0.36ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.79ms	ICMP	
5	67.14.34.38	5.01ms	ICMP	
6	4.68.62.77	4.83ms	ICMP	
7	80.239.195.62	5.89ms	ICMP	
8	62.115.125.160	5.79ms	ICMP	
9	62.115.116.41	11.89ms	UDP	80
10	62.115.123.136	43.69ms	ICMP	
11	80.91.246.74	59.90ms	ICMP	
12	62.115.113.49	74.90ms	ICMP	
13	62.115.125.7	74.73ms	ICMP	
14	62.115.12.170	75.14ms	ICMP	
15	69.25.0.74	74.63ms	ICMP	
16	69.25.5.182	75.15ms	ICMP	
17	216.52.163.130	81.01ms	ICMP	
18	173.230.231.244	75.53ms	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: 1787 seconds

Start time: Sat, Feb 20 2021, 06:37:34 GMT

End time: Sat, Feb 20 2021, 07:07:21 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
web1.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	80	1:20:14
TCP	443	1:53:23

 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	

443	https	http protocol over TLS/SSL	http 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 1021326296 with a standard deviation of 631714333. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5040 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: 30 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: 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 06:48:07 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 06:50:19 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

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 06:41:44 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 06:43:20 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 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 06:41:44 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
/tmp/	brute force
/backups	brute force
/portal/	web page
/portal/images/	web page
/Portal/	brute force
/test/	web page
/Portal/	web page
/Portal/images/	web page

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 06:48:07 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/	brute force
/portal/	web page
/portal/images/	web page
/test/	web page
/Portal/	web page
/Portal/images/	web page

Information Gathered (35)

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 Vista / Windows 2008 / Windows 7 / Windows 2012	TCP/IP Fingerprint	U3423:443


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 2 days, 22 hours, and 22 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

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

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
173.230.231.245	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, 135, 445.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.

1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100,
2102, and more.
We have omitted from this list 702 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The network handle is: WEBHOSTING-NET
Network description:
Webhosting.Net, Inc.

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The ISP network handle is: NET-216-52-163-128-1
ISP Network description:
webhosting.net INAP-MIA003-WEBHOSTING-54358

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	64.39.111.3	0.38ms	ICMP	
2	216.35.14.45	0.41ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.80ms	ICMP	
5	67.14.34.38	5.09ms	ICMP	

6	4.68.62.77	5.50ms	ICMP	
7	80.239.195.62	5.55ms	ICMP	
8	62.115.125.160	5.55ms	UDP	80
9	62.115.116.41	11.95ms	UDP	80
10	62.115.123.136	43.68ms	ICMP	
11	80.91.246.74	59.61ms	ICMP	
12	62.115.113.49	74.79ms	ICMP	
13	62.115.125.7	74.85ms	ICMP	
14	62.115.12.170	76.26ms	ICMP	
15	69.25.0.10	74.53ms	ICMP	
16	69.25.5.182	75.30ms	ICMP	
17	216.52.163.130	83.16ms	ICMP	
18	173.230.231.245	75.94ms	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: 1653 seconds

Start time: Sat, Feb 20 2021, 06:37:34 GMT

End time: Sat, Feb 20 2021, 07:05:07 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	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	443	1:52:01
TCP	8080	0:19:04
TCP	8181	0:15:51

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
443	https	http protocol over TLS/SSL	http over ssl	
8080	http-alt	HTTP Alternate (see port 80)	unknown	
8181	IpSwitch-IMail-WebStatus	IpSwitch-IMail-WebStatus	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

 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 1173399126 with a standard deviation of 578967056. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4992 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 443: 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 1 1 1
Duration: 30 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 06:44:56 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>
```

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 06:47:42 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 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 06:44:56 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

173.230.231.247 (web2.enterate.com, -) Windows Vista / Windows 2008

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 (19)

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 Vista / Windows 2008	TCP/IP Fingerprint	U3423:80

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 35 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

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

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
173.230.231.247	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, 135, 445, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-79,81-223,242-246,256-265,
280-282,309,311,318,322-325,344-351,363,369-442,444-581,587,592-593,598,
600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100, and more.
We have omitted from this list 705 higher ports to keep the report size manageable.

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The network handle is: WEBHOSTING-NET
Network description:
Webhosting.Net, Inc.

 1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:

N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

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

RESULTS:
The ISP network handle is: PNAP-12-2002
ISP Network description:
Internap Holding LLC

 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	64.39.111.3	0.39ms	ICMP	
2	216.35.14.45	0.36ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	67.14.43.82	3.74ms	ICMP	
5	67.14.34.38	4.53ms	ICMP	
6	4.68.62.77	4.87ms	ICMP	
7	80.239.195.62	5.52ms	ICMP	
8	62.115.125.160	5.68ms	ICMP	
9	62.115.116.41	11.81ms	ICMP	
10	62.115.123.136	43.69ms	ICMP	
11	80.91.246.74	59.72ms	ICMP	
12	62.115.113.49	74.81ms	ICMP	
13	62.115.125.7	74.74ms	ICMP	
14	62.115.12.170	75.13ms	ICMP	
15	69.25.0.10	74.51ms	ICMP	
16	69.25.5.182	80.76ms	ICMP	

17	*.*.*.*	0.00ms	Other	80
18	173.230.231.247	75.46ms	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: 1358 seconds

Start time: Sat, Feb 20 2021, 06:37:34 GMT

End time: Sat, Feb 20 2021, 07:00:12 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	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	80	1:50:23
TCP	443	0:04:02

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	
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

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 1025762369 with a standard deviation of 674088786. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(4996 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 2 2 2 3
Duration: 31 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</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 06:40:52 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

Appendix

Hosts Scanned (IP)

64.135.81.16-64.135.81.21, 64.135.81.24, 64.135.81.26, 64.135.81.31, 173.230.231.241-173.230.231.245, 173.230.231.247

Target distribution across scanner appliances

External : 64.135.81.16-64.135.81.31, 173.230.231.240-173.230.231.255

Hosts Not Scanned

Hosts Not Alive (IP) (17)

64.135.81.22-64.135.81.23, 64.135.81.25, 64.135.81.27-64.135.81.30, 173.230.231.240, 173.230.231.246, 173.230.231.248-173.230.231.255

Options Profile

Initial Options

Scan Settings	
Ports:	
Scanned TCP Ports:	Standard Scan
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:	Disabled
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:	Off
Ignore all TCP RST packets:	Off
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.
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.