Qualys. Community Edition

Scan Results

July 11, 2024

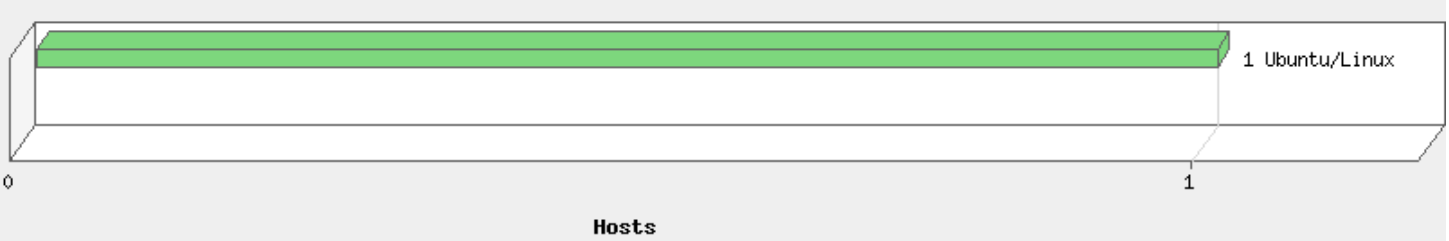
Report Summary

User Name:	Radhwen Jellali
Login Name:	tdsgb5re
Company:	TDS Global Technologies
User Role:	Manager
Address:	
City:	TUNIS.
Zip:	1082
Country:	Tunisia
Created:	07/11/2024 at 10:46:17 (GMT)
Launch Date:	07/11/2024 at 10:38:22 (GMT)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1720694302.73364
Scanner Appliances:	TDS_SCANNER (Scanner 12.18.24-1, Vulnerability Signatures 2.6.92-2)
Duration:	00:04:55
Title:	sacn ubuntu
Asset Groups:	-
IPs:	192.168.1.53
Excluded IPs:	-

Vulnerabilities by Severity

There are no known vulnerabilities for this/these systems

Operating Systems Detected



Detailed Results

192.168.1.53 (-, -) Ubuntu/Linux

Information Gathered (10)

2 Operating System Detected

QID:	45017
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/04/2024
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
Ubuntu/Linux	TCP/IP Fingerprint	U7254:7000

 2 Host Uptime Based on TCP TimeStamp Option

QID:	82063
Category:	TCP/IP
Associated CVEs:	-
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 7000, the host's uptime is 39 days, 14 hours, and 7 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

1 DNS Host Name

QID:	6
Category:	Information gathering
Associated CVEs:	-
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
192.168.1.53	No registered hostname

1 Host Scan Time - Scanner

QID:	45038
Category:	Information gathering
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/15/2022
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.

IMPACT:

N/A

SOLUTION:

N/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: 284 seconds

Start time: Thu, Jul 11 2024, 10:40:55 GMT

End time: Thu, Jul 11 2024, 10:45:39 GMT

1 Scan Activity per Port

QID:	45426
Category:	Information gathering
Associated CVEs:	-
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	7000	0:05:20

 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
Associated CVEs:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/01/2024
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
7000	VDO-Live	file server itself remote grab backdoor	unknown	

1 ICMP Replies Received

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

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	10:40:52 GMT
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 22696	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 3527	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 53	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1812	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1055	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7301	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 26084	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 13	Port Unreachable
Unreachable (type=3 code=2)	IP with High Protocol	Protocol Unreachable
Unreachable (type=3 code=3)	UDP Port 1049	Port Unreachable

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
Associated CVEs:	-
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 1172134108 with a standard deviation of 568724008. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5708 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
Associated CVEs:	-
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 7000: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 27 milli seconds

1 Host Name Not Available

QID:	82056
Category:	TCP/IP
Associated CVEs:	-
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

Vulnerabilities (1)

4 SSH Prefix Truncation Vulnerability (Terrapin) port 22/tcp

QID:	38913
Category:	General remote services
Associated CVEs:	CVE-2023-48795
Vendor Reference:	OpenSSH Advisory
Bugtraq ID:	-
Service Modified:	04/20/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

The Terrapin attack exploits weaknesses in the SSH transport layer protocol in combination with newer cryptographic algorithms and encryption modes introduced by OpenSSH over 10 years ago. Since then, these have been adopted by a wide range of SSH implementations, therefore affecting a majority of current implementations.

IMPACT:

Successful exploitation of the vulnerability may allow an attacker to downgrade the security of an SSH connection when using SSH extension negotiation. The impact in practice heavily depends on the supported extensions. Most commonly, this will impact the security of client authentication when using an RSA public key.

SOLUTION:

Customers are advised to refer to the individual vendor advisory for their operating system and install the patch released by the vendor. For more information regarding the vulnerability, please refer to Terrapin Vulnerability (https://terrapin-attack.com/)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

OpenWall Security Advisory (https://www.openwall.com/lists/oss-security/2023/12/20/3)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

packetstorm
Reference: CVE-2023-48795
Description: Terrapin SSH Connection Weakening
Link: https://packetstormsecurity.com/files/176280/Terrapin-SSH-Connection-Weakening.html

nist-nvd2
Reference: CVE-2023-48795
Description: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the ha
Link: https://www.terrapin-attack.com

nuclei-templates
Reference: CVE-2023-48795
Description: Nuclei template for CVE-2023-48795
Link: https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/main/javascript/cves/2023/CVE-2023-48795.yaml

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False

Potential Vulnerabilities (2)

5 Open Secure Sockets Layer (OpenSSL) Command Injection Vulnerability

QID:	38895
Category:	General remote services
Associated CVEs:	CVE-2022-2068
Vendor Reference:	CVE-2022-2068
Bugtraq ID:	-
Service Modified:	12/19/2023
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks.

Affected Version

OpenSSL 1.0.2 prior to 1.0.2zf (premium support customers only)
OpenSSL 1.1.1 prior to 1.1.1p
OpenSSL 3.0.0 prior to 3.0.4

IMPACT:

If successfully exploited, this vulnerability could potentially allow a command injection

SOLUTION:

Vendor has released a patch to address these vulnerabilities. Customers are advised to refer to OpenSSL Security Advisory (https://www.openssl.org/news/secadv/20220621.txt) for more information pertaining to these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

OpenSSL (https://www.openssl.org/news/secadv/20220621.txt)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable OpenSSL version detected on port 443 over TCP -
Date: Thu, 11 Jul 2024 09:15:10 GMT
Server: Apache/2.4.53 (Fedora) OpenSSL/1.1.1n mod_wsgi/4.7.1 Python/3.9
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.

</body></html>

5 Open Secure Sockets Layer (OpenSSL) Command Injection Vulnerability (CVE-2022-1292)

QID:	38936
Category:	General remote services
Associated CVEs:	CVE-2022-1292
Vendor Reference:	CVE-2022-1292
Bugtraq ID:	-
Service Modified:	05/10/2024
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:

Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks.

Affected Version

OpenSSL 1.0.2 to prior to 1.0.2ze (premium support customers).
OpenSSL 1.1.1 to prior to 1.1.1o.
OpenSSL 3.0.0 to prior to 3.0.3

IMPACT:

Successful exploitation of this vulnerability may compromise Confidentiality, Integrity, and Availability of the data.

SOLUTION:

The vendor has released a patch to address these vulnerabilities. Customers are advised to refer to OpenSSL Security Advisory (https://www.openssl.org/news/secadv/20220503.txt) for more information pertaining to these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

OpenSSL (https://www.openssl.org/news/secadv/20220503.txt)

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

github-exploits
Reference: CVE-2022-1292
Description: und3sc0n0c1d0/CVE-2022-1292 exploit repository
Link: https://github.com/und3sc0n0c1d0/CVE-2022-1292

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Vulnerable OpenSSL version detected on port 443 over TCP -
Date: Thu, 11 Jul 2024 09:15:10 GMT
Server: Apache/2.4.53 (Fedora) OpenSSL/1.1.1n mod_wsgi/4.7.1 Python/3.9
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.

</body></html>