Scan Report

December 19, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "shpcvm-1a88c.serverlet.com". The scan started at Tue Dec 19 11:46:56 2023 UTC and ended at Tue Dec 19 11:57:46 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
5.196.128.39 shpcvm-1a88c.serverlet.com	3	3	2	0	0
Total: 1	3	3	2	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 8 results selected by the filtering described above. Before filtering there were 55 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
5.196.128.39 - shpcvm-1a88c.serverlet.com	SSH	Success	Protocol SSH, Port 22, User root

2 Results per Host

2.1 5.196.128.39

Host scan start	Tue Dec 19 11:47:40 2023 UTC
Host scan end	Tue Dec 19 11:57:43 2023 UTC

Service (Port)	Threat Level
package	High
22/tcp	Medium
general/tcp	Medium
general/tcp	Low
general/icmp	Low

2.1.1 High package

High (CVSS: 7.5)
NVT: Debian: Security Advisory (DSA-5532)

Summary
The remote host is missing an update for the Debian 'openssl' package(s) announced via the DSA-5532 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libssl3
Installed version:    libssl3-3.0.11-1~deb12u1
Fixed version:      >=libssl3-3.0.11-1~deb12u2
Vulnerable package:   openssl
Installed version:    openssl-3.0.11-1~deb12u1
Fixed version:      >=openssl-3.0.11-1~deb12u2
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'openssl' package(s) on Debian 12.

Vulnerability Insight
Tony Battersby reported that incorrect cipher key and IV length processing in OpenSSL, a Secure Sockets Layer toolkit, may result in loss of confidentiality for some symmetric cipher modes.
Additional details can be found in the upstream advisory: [link moved to references]
For the stable distribution (bookworm), this problem has been fixed in version 3.0.11-1 deb12u2.
We recommend that you upgrade your openssl packages.
For the detailed security status of openssl please refer to its security tracker page at: [link moved to references]

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory (DSA-5532)`
OID:1.3.6.1.4.1.25623.1.1.1.1.2023.5532
Version used: `2023-11-13T04:20:32Z`

References
```
url: https://www.debian.org/security/2023/dsa-5532
url: https://security-tracker.debian.org/tracker/DSA-5532
url: https://www.openssl.org/news/secadv/20231024.txt
url: https://security-tracker.debian.org/tracker/openssl
cve: CVE-2023-5363
advisory_id: DSA-5532
cert-bund: WID-SEC-2023-3032
```

... continues on next page ...

... continued from previous page ...

cert-bund: WID-SEC-2023-2741
dfn-cert: DFN-CERT-2023-2624
dfn-cert: DFN-CERT-2023-2615
dfn-cert: DFN-CERT-2023-2610

High (CVSS: 8.8)
NVT: Debian: Security Advisory (DSA-5553)

Summary
The remote host is missing an update for the Debian 'postgresql-15' package(s) announced via the DSA-5553 advisory.

Quality of Detection: 97

Vulnerability Detection Result
Vulnerable package: libpq5
Installed version: libpq5-15.3-0+deb12u1
Fixed version: >=libpq5-15.5-0+deb12u1

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'postgresql-15' package(s) on Debian 12.

Vulnerability Insight
Several vulnerabilities have been discovered in the PostgreSQL database system.
CVE-2023-5868
Jingzhou Fu discovered a memory disclosure flaw in aggregate function calls.
CVE-2023-5869
Pedro Gallegos reported integer overflow flaws resulting in buffer overflows in the array modification functions.
CVE-2023-5870
Hemanth Sandrana and Mahendrakar Srinivasarao reported that the pg_cancel_backend role can signal certain superuser processes, potentially resulting in denial of service.
CVE-2023-39417
Micah Gate, Valerie Woolard, Tim Carey-Smith, and Christoph Berg reported that an extension script using @substitutions@ within quoting may allow to perform an SQL injection for an attacker having database-level CREATE privileges.
CVE-2023-39418
Dean Rasheed reported that the MERGE command fails to enforce UPDATE or SELECT row security policies.
For the stable distribution (bookworm), these problems have been fixed in version 15.5-0+deb12u1.
We recommend that you upgrade your postgresql-15 packages.

... continues on next page ...

... continued from previous page ...

For the detailed security status of postgresql-15 please refer to its security tracker page at: [link moved to references]

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory (DSA-5553)`
OID:1.3.6.1.4.1.25623.1.1.1.1.2023.5553
Version used: `2023-12-15T04:21:33Z`

References
`url: https://www.debian.org/security/2023/dsa-5553`
`url: https://security-tracker.debian.org/tracker/DSA-5553`
`url: https://security-tracker.debian.org/tracker/postgresql-15`
`cve: CVE-2023-39417`
`cve: CVE-2023-39418`
`cve: CVE-2023-5868`
`cve: CVE-2023-5869`
`cve: CVE-2023-5870`
`advisory_id: DSA-5553`
`cert-bund: WID-SEC-2023-3041`
`cert-bund: WID-SEC-2023-2873`
`cert-bund: WID-SEC-2023-2038`
`dfn-cert: DFN-CERT-2023-3132`
`dfn-cert: DFN-CERT-2023-3125`
`dfn-cert: DFN-CERT-2023-2983`
`dfn-cert: DFN-CERT-2023-2813`
`dfn-cert: DFN-CERT-2023-2812`
`dfn-cert: DFN-CERT-2023-2788`
`dfn-cert: DFN-CERT-2023-1855`

High (CVSS: 7.5)
NVT: Debian: Security Advisory (DSA-5570)

Summary
The remote host is missing an update for the Debian 'nghttp2' package(s) announced via the DSA-5570 advisory.

Quality of Detection: 97

Vulnerability Detection Result
```
Vulnerable package:   libnghttp2-14
Installed version:    libnghttp2-14-1.52.0-1
Fixed version:      >=libnghttp2-14-1.52.0-1+deb12u1
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'nghttp2' package(s) on Debian 11, Debian 12.

Vulnerability Insight
It was discovered that libnghttp2, a library implementing the HTTP/2 protocol, handled request cancellation incorrectly. This could result in denial of service.
For the oldstable distribution (bullseye), this problem has been fixed in version 1.43.0-1+deb11u1.
For the stable distribution (bookworm), this problem has been fixed in version 1.52.0-1+deb12u1.
We recommend that you upgrade your nghttp2 packages.
For the detailed security status of nghttp2 please refer to its security tracker page at: [link moved to references]

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory (DSA-5570)`
OID:1.3.6.1.4.1.25623.1.1.1.1.2023.5570
Version used: `2023-12-04T04:22:47Z`

References
`url: https://www.debian.org/security/2023/dsa-5570`
`url: https://security-tracker.debian.org/tracker/DSA-5570`
`url: https://security-tracker.debian.org/tracker/nghttp2`
`cve: CVE-2023-44487`
`advisory_id: DSA-5570`
`cert-bund: WID-SEC-2023-2993`
`cert-bund: WID-SEC-2023-2788`
`cert-bund: WID-SEC-2023-2723`
`cert-bund: WID-SEC-2023-2655`
`cert-bund: WID-SEC-2023-2628`
`cert-bund: WID-SEC-2023-2627`
`cert-bund: WID-SEC-2023-2618`
`cert-bund: WID-SEC-2023-2611`
`cert-bund: WID-SEC-2023-2606`
`dfn-cert: DFN-CERT-2023-3124`
`dfn-cert: DFN-CERT-2023-3119`
`dfn-cert: DFN-CERT-2023-3073`
`dfn-cert: DFN-CERT-2023-3059`
`dfn-cert: DFN-CERT-2023-3035`
`dfn-cert: DFN-CERT-2023-3007`
`dfn-cert: DFN-CERT-2023-2996`
`dfn-cert: DFN-CERT-2023-2991`
`dfn-cert: DFN-CERT-2023-2971`
`dfn-cert: DFN-CERT-2023-2959`
`dfn-cert: DFN-CERT-2023-2912`
`dfn-cert: DFN-CERT-2023-2892`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2023-2882
dfn-cert: DFN-CERT-2023-2876
dfn-cert: DFN-CERT-2023-2864
dfn-cert: DFN-CERT-2023-2851
dfn-cert: DFN-CERT-2023-2849
dfn-cert: DFN-CERT-2023-2787
dfn-cert: DFN-CERT-2023-2785
dfn-cert: DFN-CERT-2023-2730
dfn-cert: DFN-CERT-2023-2729
dfn-cert: DFN-CERT-2023-2708
dfn-cert: DFN-CERT-2023-2696
dfn-cert: DFN-CERT-2023-2695
dfn-cert: DFN-CERT-2023-2680
dfn-cert: DFN-CERT-2023-2677
dfn-cert: DFN-CERT-2023-2675
dfn-cert: DFN-CERT-2023-2670
dfn-cert: DFN-CERT-2023-2666
dfn-cert: DFN-CERT-2023-2646
dfn-cert: DFN-CERT-2023-2637
dfn-cert: DFN-CERT-2023-2636
dfn-cert: DFN-CERT-2023-2635
dfn-cert: DFN-CERT-2023-2623
dfn-cert: DFN-CERT-2023-2603
dfn-cert: DFN-CERT-2023-2600
dfn-cert: DFN-CERT-2023-2599
dfn-cert: DFN-CERT-2023-2597
dfn-cert: DFN-CERT-2023-2596
dfn-cert: DFN-CERT-2023-2595
dfn-cert: DFN-CERT-2023-2590
dfn-cert: DFN-CERT-2023-2589
dfn-cert: DFN-CERT-2023-2586
dfn-cert: DFN-CERT-2023-2585
dfn-cert: DFN-CERT-2023-2572
dfn-cert: DFN-CERT-2023-2571
dfn-cert: DFN-CERT-2023-2568
dfn-cert: DFN-CERT-2023-2564
dfn-cert: DFN-CERT-2023-2556
dfn-cert: DFN-CERT-2023-2555
dfn-cert: DFN-CERT-2023-2552
dfn-cert: DFN-CERT-2023-2549
dfn-cert: DFN-CERT-2023-2547
dfn-cert: DFN-CERT-2023-2528
dfn-cert: DFN-CERT-2023-2522
dfn-cert: DFN-CERT-2023-2512
dfn-cert: DFN-CERT-2023-2504
dfn-cert: DFN-CERT-2023-2501
dfn-cert: DFN-CERT-2023-2487

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2023-2469
dfn-cert: DFN-CERT-2023-2468
dfn-cert: DFN-CERT-2023-2459
dfn-cert: DFN-CERT-2023-2457
dfn-cert: DFN-CERT-2023-2453
dfn-cert: DFN-CERT-2023-2450
dfn-cert: DFN-CERT-2023-2449
dfn-cert: DFN-CERT-2023-2439
```

[return to 5.196.128.39]

2.1.2 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------
diffie-hellman-group-exchange-sha1 | Using SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: 2023-10-12T05:05:32Z

References
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142
url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
url: https://www.rfc-editor.org/rfc/rfc6194
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5

[return to 5.196.128.39]

2.1.3 Medium general/tcp

Medium (CVSS: 5.6)
NVT: Missing Linux Kernel mitigations for 'MDS - Microarchitectural Data Sampling' hardware vulnerabilities

Product detection result
cpe:/a:linux:kernel
Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili
↪ties (OID: 1.3.6.1.4.1.25623.1.0.108765)

Summary
The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'MDS - Microarchitectural Data Sampling' hardware vulnerabilities.

Quality of Detection: 80

Vulnerability Detection Result
The Linux Kernel on the remote host is missing the mitigation for the "mds" hard
↪ware vulnerabilities as reported by the sysfs interface:
sysfs file checked | Linux Kernel status (SSH response)

↪---
/sys/devices/system/cpu/vulnerabilities/mds | Vulnerable: Clear CPU buffers atte
↪mpted, no microcode; SMT Host state unknown
Notes on the "Linux Kernel status (SSH response)" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for th

... continues on next page ...

... continued from previous page ...

```
↪is specific vulnerability is missing. This means the current Linux Kernel does
↪n't know this vulnerability yet. Based on this it is assumed that it doesn't p
↪rovide any mitigation and that the target system is vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported d
↪irectly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Solution:
Solution type: VendorFix
The following solutions exist:
- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it
- Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration)
Additional possible mitigations (if provided by the vendor) are to:
- install a Microcode update
- update the BIOS of the Mainboard
Note: Please create an override for this result if the sysfs file is not available but other mitigations like a Microcode update is already in place.

Vulnerability Detection Method
Checks previous gathered information on the mitigation status reported by the Linux Kernel.
Details: `Missing Linux Kernel mitigations for 'MDS - Microarchitectural Data Sampling' h.
↪..`
OID:1.3.6.1.4.1.25623.1.0.108840
Version used: `2023-08-14T05:05:34Z`

Product Detection Result
Product: `cpe:/a:linux:kernel`
Method: `Detection of Linux Kernel mitigation status for hardware vulnerabilities`
OID: 1.3.6.1.4.1.25623.1.0.108765)

References
`cve: CVE-2018-12126`
`cve: CVE-2018-12130`
`cve: CVE-2018-12127`
`cve: CVE-2019-11091`
`url: https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/mds.html`
`cert-bund: WID-SEC-2023-1692`
`cert-bund: CB-K19/0414`
`dfn-cert: DFN-CERT-2020-1041`
`dfn-cert: DFN-CERT-2020-0069`
`dfn-cert: DFN-CERT-2020-0048`
`dfn-cert: DFN-CERT-2019-2374`
`dfn-cert: DFN-CERT-2019-2214`
`dfn-cert: DFN-CERT-2019-1985`

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2019-1767
dfn-cert: DFN-CERT-2019-1414
dfn-cert: DFN-CERT-2019-1235
dfn-cert: DFN-CERT-2019-1200
dfn-cert: DFN-CERT-2019-1172
dfn-cert: DFN-CERT-2019-1151
dfn-cert: DFN-CERT-2019-1149
dfn-cert: DFN-CERT-2019-1122
dfn-cert: DFN-CERT-2019-1083
dfn-cert: DFN-CERT-2019-1036
dfn-cert: DFN-CERT-2019-1032
dfn-cert: DFN-CERT-2019-1026
dfn-cert: DFN-CERT-2019-1025
dfn-cert: DFN-CERT-2019-1024
dfn-cert: DFN-CERT-2019-1017
dfn-cert: DFN-CERT-2019-1012
dfn-cert: DFN-CERT-2019-1009
dfn-cert: DFN-CERT-2019-1005
dfn-cert: DFN-CERT-2019-1004
dfn-cert: DFN-CERT-2019-1003
dfn-cert: DFN-CERT-2019-1002
dfn-cert: DFN-CERT-2019-0994
dfn-cert: DFN-CERT-2019-0990
dfn-cert: DFN-CERT-2019-0989
dfn-cert: DFN-CERT-2019-0988
dfn-cert: DFN-CERT-2019-0987
dfn-cert: DFN-CERT-2019-0986
dfn-cert: DFN-CERT-2019-0977
dfn-cert: DFN-CERT-2019-0974
dfn-cert: DFN-CERT-2019-0971
dfn-cert: DFN-CERT-2019-0969
dfn-cert: DFN-CERT-2019-0950
dfn-cert: DFN-CERT-2018-2399
```

Medium (CVSS: 5.5)
NVT: Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities

Product detection result

```
cpe:/a:linux:kernel
Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili
↪ties (OID: 1.3.6.1.4.1.25623.1.0.108765)
```

Summary

The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'SSB - Speculative Store Bypass' hardware vulnerabilities.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "spec_stor
↪e_bypass" hardware vulnerabilities as reported by the sysfs interface:
sysfs file checked                                          | Linux Kernel status
↪(SSH response)
-------------------------------------------------------------------------------
↪--------------
/sys/devices/system/cpu/vulnerabilities/spec_store_bypass | Vulnerable
Notes on the "Linux Kernel status (SSH response)" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for th
↪is specific vulnerability is missing. This means the current Linux Kernel does
↪n't know this vulnerability yet. Based on this it is assumed that it doesn't p
↪rovide any mitigation and that the target system is vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported d
↪irectly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Solution:
Solution type: VendorFix
The following solutions exist:
- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it
- Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration)
Additional possible mitigations (if provided by the vendor) are to:
- install a Microcode update
- update the BIOS of the Mainboard
Note: Please create an override for this result if the sysfs file is not available but other mitigations like a Microcode update is already in place.

Vulnerability Detection Method
Checks previous gathered information on the mitigation status reported by the Linux Kernel.
Details: `Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware .
↪..`
OID:1.3.6.1.4.1.25623.1.0.108842
Version used: `2023-08-14T05:05:34Z`

Product Detection Result
Product: `cpe:/a:linux:kernel`
Method: `Detection of Linux Kernel mitigation status for hardware vulnerabilities`
OID: 1.3.6.1.4.1.25623.1.0.108765)

References

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2018-3639
url: https://www.kernel.org/doc/html/latest/admin-guide/hw-vuln/index.html
cert-bund: WID-SEC-2023-2917
cert-bund: WID-SEC-2023-2072
cert-bund: CB-K19/0271
cert-bund: CB-K19/0047
cert-bund: CB-K18/1050
cert-bund: CB-K18/0686
cert-bund: CB-K18/0682
dfn-cert: DFN-CERT-2023-1947
dfn-cert: DFN-CERT-2023-1924
dfn-cert: DFN-CERT-2023-1904
dfn-cert: DFN-CERT-2023-1900
dfn-cert: DFN-CERT-2021-2551
dfn-cert: DFN-CERT-2020-1987
dfn-cert: DFN-CERT-2020-1935
dfn-cert: DFN-CERT-2020-1912
dfn-cert: DFN-CERT-2020-1783
dfn-cert: DFN-CERT-2020-1473
dfn-cert: DFN-CERT-2020-1078
dfn-cert: DFN-CERT-2019-0622
dfn-cert: DFN-CERT-2019-0544
dfn-cert: DFN-CERT-2019-0286
dfn-cert: DFN-CERT-2019-0258
dfn-cert: DFN-CERT-2019-0168
dfn-cert: DFN-CERT-2019-0108
dfn-cert: DFN-CERT-2019-0069
dfn-cert: DFN-CERT-2019-0059
dfn-cert: DFN-CERT-2018-2554
dfn-cert: DFN-CERT-2018-2441
dfn-cert: DFN-CERT-2018-2399
dfn-cert: DFN-CERT-2018-2349
dfn-cert: DFN-CERT-2018-2302
dfn-cert: DFN-CERT-2018-2217
dfn-cert: DFN-CERT-2018-2213
dfn-cert: DFN-CERT-2018-1982
dfn-cert: DFN-CERT-2018-1929
dfn-cert: DFN-CERT-2018-1869
dfn-cert: DFN-CERT-2018-1767
dfn-cert: DFN-CERT-2018-1734
dfn-cert: DFN-CERT-2018-1658
dfn-cert: DFN-CERT-2018-1651
dfn-cert: DFN-CERT-2018-1627
dfn-cert: DFN-CERT-2018-1624
dfn-cert: DFN-CERT-2018-1500
dfn-cert: DFN-CERT-2018-1494
dfn-cert: DFN-CERT-2018-1493
```

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2018-1446
dfn-cert: DFN-CERT-2018-1435
dfn-cert: DFN-CERT-2018-1374
dfn-cert: DFN-CERT-2018-1353
dfn-cert: DFN-CERT-2018-1351
dfn-cert: DFN-CERT-2018-1323
dfn-cert: DFN-CERT-2018-1304
dfn-cert: DFN-CERT-2018-1270
dfn-cert: DFN-CERT-2018-1260
dfn-cert: DFN-CERT-2018-1234
dfn-cert: DFN-CERT-2018-1228
dfn-cert: DFN-CERT-2018-1205
dfn-cert: DFN-CERT-2018-1183
dfn-cert: DFN-CERT-2018-1151
dfn-cert: DFN-CERT-2018-1129
dfn-cert: DFN-CERT-2018-1117
dfn-cert: DFN-CERT-2018-1105
dfn-cert: DFN-CERT-2018-1042
dfn-cert: DFN-CERT-2018-1041
dfn-cert: DFN-CERT-2018-1025
dfn-cert: DFN-CERT-2018-1023
dfn-cert: DFN-CERT-2018-0993
dfn-cert: DFN-CERT-2018-0992
dfn-cert: DFN-CERT-2018-0991
dfn-cert: DFN-CERT-2018-0987
dfn-cert: DFN-CERT-2018-0976
dfn-cert: DFN-CERT-2018-0973
dfn-cert: DFN-CERT-2018-0972
dfn-cert: DFN-CERT-2018-0970
dfn-cert: DFN-CERT-2018-0966
```

[return to 5.196.128.39]

2.1.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection: 80

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
```

... continues on next page ...

... continued from previous page ...

```
Packet 1: 4007639691
Packet 2: 4007640782
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-08-01T13:29:10Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`

[return to 5.196.128.39]

2.1.5 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

... continues on next page ...

... continued from previous page ...

Quality of Detection: 80

Vulnerability Detection Result
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2023-05-11T09:09:33Z

References
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[return to 5.196.128.39]