

Scan Report

July 4, 2024

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 “Scan Bizness”. The scan started at Thu Jul 4 20:13:59 2024 UTC and ended at Thu Jul 4 22:43:21 2024 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	2
2	Results per Host	2
2.1	10.10.11.252	2
2.1.1	Medium 443/tcp	2
2.1.2	Low general/icmp	6
2.1.3	Low 22/tcp	7
2.1.4	Low general/tcp	8

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.10.11.252 business.htb	0	1	3	0	0
Total: 1	0	1	3	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 4 results selected by the filtering described above. Before filtering there were 70 results.

2 Results per Host

2.1 10.10.11.252

Host scan start Thu Jul 4 20:14:32 2024 UTC

Host scan end Thu Jul 4 22:43:16 2024 UTC

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

2.1.1 Medium 443/tcp

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

cpe:/a:ietf:transport_layer_security:1.0

Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)

... continues on next page ...

...continued from previous page ...
Summary It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Quality of Detection: 98
Vulnerability Detection Result In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.
Solution: Solution type: Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
Affected Software/OS All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.
Vulnerability Insight The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)
Vulnerability Detection Method Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2024-06-14T05:05:48Z
Product Detection Result Product: cpe:/a:ietf:transport_layer_security:1.0 Method: SSL/TLS: Version Detection OID: 1.3.6.1.4.1.25623.1.0.105782)
... continues on next page ...

...continued from previous page...

References

cve: CVE-2011-3389
cve: CVE-2015-0204
url: <https://ssl-config.mozilla.org/>
url: <https://bettercrypto.org/>
url: <https://datatracker.ietf.org/doc/rfc8996/>
url: <https://vnhacker.blogspot.com/2011/09/beast.html>
url: <https://web.archive.org/web/20201108095603/https://censys.io/blog/freak>
url: <https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters>
↔-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884

...continues on next page...

...continued from previous page ...

dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126

...continues on next page ...

...continued from previous page ...

```

dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482

```

[\[return to 10.10.11.252 \]](#)

2.1.2 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary

The remote host responded to an ICMP timestamp request.

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

... continues on next page ...

...continued from previous page ...
- 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

[\[return to 10.10.11.252 \]](#)

2.1.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)
Product detection result cpe:/a:ietf:secure_shell_protocol Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565 ↔)
Summary The remote SSH server is configured to allow / support weak MAC algorithm(s).
Quality of Detection: 80
Vulnerability Detection Result The remote SSH server supports the following weak client-to-server MAC algorithm ... continues on next page ...

...continued from previous page ...
<pre>↔(s): umac-64-etm@openssh.com umac-64@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm ↔(s): umac-64-etm@openssh.com umac-64@openssh.com</pre>
<p>Solution:</p> <p>Solution type: Mitigation</p> <p>Disable the reported weak MAC algorithm(s).</p>
<p>Vulnerability Detection Method</p> <p>Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.</p> <p>Currently weak MAC algorithms are defined as the following:</p> <ul style="list-style-type: none">- MD5 based algorithms- 96-bit based algorithms- 64-bit based algorithms- 'none' algorithm <p>Details: Weak MAC Algorithm(s) Supported (SSH)</p> <p>OID:1.3.6.1.4.1.25623.1.0.105610</p> <p>Version used: 2024-06-14T05:05:48Z</p>
<p>Product Detection Result</p> <p>Product: cpe:/a:ietf:secure_shell_protocol</p> <p>Method: SSH Protocol Algorithms Supported</p> <p>OID: 1.3.6.1.4.1.25623.1.0.105565)</p>
<p>References</p> <p>url: https://www.rfc-editor.org/rfc/rfc6668</p> <p>url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4</p>

[\[return to 10.10.11.252 \]](#)

2.1.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
<p>Summary</p> <p>The remote host implements TCP timestamps and therefore allows to compute the uptime.</p>
... continues on next page ...

...continued from previous page...

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:

Packet 1: 73908192

Packet 2: 73909354

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: 2023-12-15T16:10:08Z

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/download/details.aspx?id=9152>

url: <https://www.fortiguard.com/psirt/FG-IR-16-090>

[\[return to 10.10.11.252 \]](#)

This file was automatically generated.