Scan Report

August 7, 2025

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 "Full vulnerability scan - router". The scan started at Thu Aug 7 09:48:39 2025 UTC and ended at Thu Aug 7 15:04:19 2025 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
192.168.31.1	0	2	0	0	0
Total: 1	0	2	0	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 2 results selected by the filtering described above. Before filtering there were 34 results.

2 Results per Host

2.1 192.168.31.1

Host scan start	Thu Aug 7 09:49:26 2025 UTC
Host scan end	Thu Aug 7 15:04:12 2025 UTC

Service (Port)	Threat Level
443/tcp	Medium

2.1.1 Medium 443/tcp

Medium (CVSS: 5.8)

NVT: SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)

Summary
The remote SSL/TLS service is prone to a man-in-the-middle (MITM) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
`Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an`

. . . continues on next page . . .

... continued from previous page ...

```
↪ existing / already established SSL/TLS connection
------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.2          | 2
```

Impact
A remote, unauthenticated attacker may be able to inject an arbitrary amount of chosen plaintext into the beginning of the application protocol stream. This could allow and attacker to issue HTTP requests, or take action impersonating the user, among other consequences.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
General solution options are:
- remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service
- enable Safe/Secure renegotiation (RFC5746) for the affected SSL/TLS service

Affected Software/OS
The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products.

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly associate renegotiation handshakes with an existing connection, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a 'plaintext injection' attack, aka the 'Project Mogul' issue.

Vulnerability Detection Method
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)`
OID:1.3.6.1.4.1.25623.1.0.117758
Version used: `2024-09-27T05:05:23Z`

References
`cve: CVE-2009-3555`
`url: https://blog.g-sec.lu/2009/11/tls-sslv3-renegotiation-vulnerability.html`
`url: https://www.g-sec.lu/practicaltls.pdf`
`url: https://www.kb.cert.org/vuls/id/120541`
`url: https://orchilles.com/ssl-renegotiation-dos/`
`url: https://lwn.net/Articles/362234/`
`url: https://kb.fortinet.com/kb/documentLink.do?externalID=FD36385`
`url: https://datatracker.ietf.org/doc/html/rfc5746`

... continues on next page ...

... continued from previous page ...

```
url: https://mailarchive.ietf.org/arch/msg/tls/Y1O3HUcq9T94rMLCGPTTozURtSI/
cert-bund: CB-K17/1878
cert-bund: CB-K17/1642
cert-bund: CB-K15/0637
dfn-cert: DFN-CERT-2017-1960
dfn-cert: DFN-CERT-2017-1722
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2013-0321
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-0828
dfn-cert: DFN-CERT-2012-0613
dfn-cert: DFN-CERT-2011-1720
dfn-cert: DFN-CERT-2011-1138
dfn-cert: DFN-CERT-2011-1137
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0700
dfn-cert: DFN-CERT-2011-0321
dfn-cert: DFN-CERT-2011-0193
dfn-cert: DFN-CERT-2011-0185
dfn-cert: DFN-CERT-2011-0181
dfn-cert: DFN-CERT-2011-0116
dfn-cert: DFN-CERT-2011-0021
dfn-cert: DFN-CERT-2011-0020
dfn-cert: DFN-CERT-2011-0019
dfn-cert: DFN-CERT-2010-1762
dfn-cert: DFN-CERT-2010-1731
dfn-cert: DFN-CERT-2010-1710
dfn-cert: DFN-CERT-2010-1702
dfn-cert: DFN-CERT-2010-1650
dfn-cert: DFN-CERT-2010-1647
dfn-cert: DFN-CERT-2010-1527
dfn-cert: DFN-CERT-2010-1500
dfn-cert: DFN-CERT-2010-1439
dfn-cert: DFN-CERT-2010-1424
dfn-cert: DFN-CERT-2010-1406
dfn-cert: DFN-CERT-2010-1405
dfn-cert: DFN-CERT-2010-1387
dfn-cert: DFN-CERT-2010-1385
dfn-cert: DFN-CERT-2010-1380
dfn-cert: DFN-CERT-2010-1368
dfn-cert: DFN-CERT-2010-1293
dfn-cert: DFN-CERT-2010-1227
dfn-cert: DFN-CERT-2010-1052
dfn-cert: DFN-CERT-2010-1009
dfn-cert: DFN-CERT-2010-1000
dfn-cert: DFN-CERT-2010-0899
dfn-cert: DFN-CERT-2010-0859
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2010-0833
dfn-cert: DFN-CERT-2010-0815
dfn-cert: DFN-CERT-2010-0775
dfn-cert: DFN-CERT-2010-0729
dfn-cert: DFN-CERT-2010-0725
dfn-cert: DFN-CERT-2010-0707
dfn-cert: DFN-CERT-2010-0705
dfn-cert: DFN-CERT-2010-0669
dfn-cert: DFN-CERT-2010-0639
dfn-cert: DFN-CERT-2010-0619
dfn-cert: DFN-CERT-2010-0618
dfn-cert: DFN-CERT-2010-0603
dfn-cert: DFN-CERT-2010-0586
dfn-cert: DFN-CERT-2010-0579
dfn-cert: DFN-CERT-2010-0562
dfn-cert: DFN-CERT-2010-0558
dfn-cert: DFN-CERT-2010-0544
dfn-cert: DFN-CERT-2010-0539
dfn-cert: DFN-CERT-2010-0525
dfn-cert: DFN-CERT-2010-0504
dfn-cert: DFN-CERT-2010-0498
dfn-cert: DFN-CERT-2010-0491
dfn-cert: DFN-CERT-2010-0488
dfn-cert: DFN-CERT-2010-0485
dfn-cert: DFN-CERT-2010-0456
dfn-cert: DFN-CERT-2010-0455
dfn-cert: DFN-CERT-2010-0451
dfn-cert: DFN-CERT-2010-0413
dfn-cert: DFN-CERT-2010-0411
dfn-cert: DFN-CERT-2010-0410
dfn-cert: DFN-CERT-2010-0407
dfn-cert: DFN-CERT-2010-0406
dfn-cert: DFN-CERT-2010-0405
dfn-cert: DFN-CERT-2010-0388
dfn-cert: DFN-CERT-2010-0370
dfn-cert: DFN-CERT-2010-0339
dfn-cert: DFN-CERT-2010-0303
dfn-cert: DFN-CERT-2010-0273
dfn-cert: DFN-CERT-2010-0201
dfn-cert: DFN-CERT-2010-0166
dfn-cert: DFN-CERT-2010-0050
dfn-cert: DFN-CERT-2010-0030
dfn-cert: DFN-CERT-2009-1833
dfn-cert: DFN-CERT-2009-1821
dfn-cert: DFN-CERT-2009-1820
dfn-cert: DFN-CERT-2009-1809
dfn-cert: DFN-CERT-2009-1805

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2009-1757
dfn-cert: DFN-CERT-2009-1755
dfn-cert: DFN-CERT-2009-1725
dfn-cert: DFN-CERT-2009-1719
dfn-cert: DFN-CERT-2009-1689
dfn-cert: DFN-CERT-2009-1688
dfn-cert: DFN-CERT-2009-1654
dfn-cert: DFN-CERT-2009-1653
dfn-cert: DFN-CERT-2009-1646
dfn-cert: DFN-CERT-2009-1643
dfn-cert: DFN-CERT-2009-1630
dfn-cert: DFN-CERT-2009-1623
dfn-cert: DFN-CERT-2009-1603
dfn-cert: DFN-CERT-2009-1602
dfn-cert: DFN-CERT-2009-1584
dfn-cert: DFN-CERT-2009-1578
```

Medium (CVSS: 5.0)

NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Summary
The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
-------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.2          | 10
```

Impact
The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:
Solution type: VendorFix
Users should contact their vendors for specific patch information.
A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight
The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.
Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:
> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.
Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method
Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.
Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`
OID:1.3.6.1.4.1.25623.1.0.117761
Version used: `2024-09-27T05:05:23Z`

References
`cve: CVE-2011-1473`
`cve: CVE-2011-5094`
`url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego`
`↪tiation-dos/`
`url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/`
`url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation`
`url: https://www.openwall.com/lists/oss-security/2011/07/08/2`
`cert-bund: WID-SEC-2024-1591`
`cert-bund: WID-SEC-2024-0796`
`cert-bund: WID-SEC-2023-1435`
`cert-bund: CB-K17/0980`
`cert-bund: CB-K17/0979`
`cert-bund: CB-K14/0772`
`cert-bund: CB-K13/0915`
`cert-bund: CB-K13/0462`
`dfn-cert: DFN-CERT-2025-0933`
`dfn-cert: DFN-CERT-2017-1013`
`dfn-cert: DFN-CERT-2017-1012`
`dfn-cert: DFN-CERT-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`
`dfn-cert: DFN-CERT-2012-1112`

[return to 192.168.31.1]