Scan Report

October 13, 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 "Ataque MITM". The scan started at Mon Oct 13 12:07:55 2025 UTC and ended at Mon Oct 13 13:26:40 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
192.168.1.1 livebox	0	8	2	0	0
Total: 1	0	8	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 10 results selected by the filtering described above. Before filtering there were 90 results.

2 Results per Host

2.1 192.168.1.1

Host scan start	Mon Oct 13 12:08:40 2025 UTC
Host scan end	Mon Oct 13 13:26:37 2025 UTC

Service (Port)	Threat Level
443/tcp	Medium
8443/tcp	Medium
80/tcp	Medium
general/icmp	Low
general/tcp	Low

2.1.1 Medium 443/tcp

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.

. . . continues on next page . . .

... continued from previous page ...

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

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/
```

... continues on next page ...

... continued from previous page ...

```
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-2014-0809
dfn-cert: DFN-CERT-2013-1928
```

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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-2014-0809`
`dfn-cert: DFN-CERT-2013-1928`

[return to 192.168.1.1]

2.1.2 Medium 8443/tcp

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Product detection result
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`

... continues on next page ...

... continued from previous page ...

↪802067)

Summary
This routine reports all weak SSL/TLS cipher suites accepted by a service.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA

Impact
This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
All services providing an encrypted communication using weak SSL/TLS cipher suites.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Checks previous collected cipher suites.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2025-03-27T05:38:50Z

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

References
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://ssl-config.mozilla.org
url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel
↪ines/TG02102/BSI-TR-02102-1.html
url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/
↪TLS-Protokoll/TLS-Protokoll_node.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch
↪eRichtlinien/TR03116/BSI-TR-03116-4.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes
↪tstandard_BSI_TLS_Version_2_4.html
url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059

... continues on next page ...

... continued from previous page ...

```
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2014-0977
```

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.

... continues on next page ...

... continued from previous page ...

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
-------------------------------------------------------------------------------
↪-----------------------------------------------
TLSv1.0          | 10
TLSv1.1          | 10
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

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/
```

... continues on next page ...

... continued from previous page ...

```
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-2014-0809
dfn-cert: DFN-CERT-2013-1928
```

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
--------------------------------------------------------------------------------
↪-------------------------------------------------
TLSv1.0          | 10
TLSv1.1          | 10
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-2014-0809
dfn-cert: DFN-CERT-2013-1928

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 (QoD): 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 resources supporting you with this task.

Affected Software/OS
- All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols
- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder
- CVE-2024-41270: Gorush v1.18.4
- CVE-2025-3200: Multiple products from Wiesemann & Theis

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
Checks 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: `2025-04-30T05:39:51Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`

... continues on next page ...

... continued from previous page ...

OID: 1.3.6.1.4.1.25623.1.0.105782)

References

cve: CVE-2011-3389
cve: CVE-2015-0204
cve: CVE-2023-41928
cve: CVE-2024-41270
cve: CVE-2025-3200
url: https://ssl-config.mozilla.org
url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel
↪ines/TG02102/BSI-TR-02102-1.html
url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/
↪TLS-Protokoll/TLS-Protokoll_node.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch
↪eRichtlinien/TR03116/BSI-TR-03116-4.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes
↪tstandard_BSI_TLS_Version_2_4.html
url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
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://certvde.com/en/advisories/VDE-2025-031/
url: https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc
url: https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273
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

... continues on next page ...

... continued from previous page ...

```
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-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-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
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 192.168.1.1]

2.1.3 Medium 80/tcp

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following input fields were identified (URL:input name):
http://localdevice.abrstream.tech/login.htm:ui_pws

... continues on next page ...

... continued from previous page ...

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The following input fields were identified (URL:input name):`

... continues on next page ...

... continued from previous page ...

http://livebox/login.htm:ui_pws

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: 2023-09-07T05:05:21Z

References
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html

[return to 192.168.1.1]

2.1.4 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 (QoD): 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: 2025-01-21T05:37:33Z

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 192.168.1.1]

2.1.5 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 (QoD): 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: 15411542
Packet 2: 15411650
```

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/d
```

... continues on next page ...

... continued from previous page ...

```
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 192.168.1.1]
