Scan Report

September 15, 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 "lab-scan". The scan started at Mon Sep 15 12:58:56 2025 UTC and ended at Mon Sep 15 14:05:34 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
10.0.2.15 lab-virtualbox.net	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 248 results.

2 Results per Host

2.1 10.0.2.15

Host scan start   Mon Sep 15 12:59:34 2025 UTC
Host scan end   Mon Sep 15 14:05:28 2025 UTC

Service (Port)	Threat Level
25/tcp	Medium

2.1.1 Medium 25/tcp

Medium (CVSS: 5.0)

NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Quality of Detection (QoD): 99%

. . . continues on next page . . .

Vulnerability Detection Result
`'VRFY root' produces the following answer: 252 2.0.0 root`

Solution:
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `2023-10-31T05:06:37Z`

References
url: `http://cr.yp.to/smtp/vrfy.html`

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)`

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`
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
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
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
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 10.0.2.15]

This file was automatically generated.