I Summary

==========

This document reports on the results of an automatic security scan.

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.

All dates are displayed using the timezone "Coordinated Universal Time",

which is abbreviated "UTC".

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.

Notes are included in the report.Information on overrides is 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 26 results selected by the

filtering described above. Before filtering there were 264 results.

Scan started: Fri Oct 16 12:16:23 2022 UTC

Scan ended: Fri Oct 16 05:34:44 2022 UTC

Task: VEROLT

Host Summary

****

Host	High	Medium	Low	Log	False Positive
43.255.154.114	0	25	1	0	0
114.154.255.43.host.secureserver.net					
Total: 1	0	25	1	0	0

II Results per Host

==========

Host 43.255.154.114

****

Scanning of this host started at: Fri Oct 14 03:15:41 2022 UTC

Number of results: 26

Port Summary for Host 43.255.154.114

Service (Port)	Threat Level
143/tcp	Medium
995/tcp	Medium
110/tcp	Medium
2087/tcp	Medium
2078/tcp	Medium
21/tcp	Medium
22/tcp	Medium
587/tcp	Medium
443/tcp	Medium
993/tcp	Medium
80/tcp	Medium
2096/tcp	Medium

Security Issues for Host 43.255.154.114

Issue

NVT: SSL/TLS: Missing `secure` Cookie Attribute

OID: 1.3.6.1.4.1.25623.1.0.902661

Threat: Medium (CVSS: 6.4)

Port: 2096/tcp

Summary:

a server with SSL/TLS is prone to an information disclosure vulnerability.

Vulnerability Detection Result:

The cookies:

Set-Cookie: Horde=***replaced***; HttpOnly; domain=.114.154.255.43.host.securese!

rver.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096

Set-Cookie: horde_secret_key=***replaced***; HttpOnly; domain=.114.154.255.43.ho!

st.secureserver.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096

are missing the "secure" attribute.

Solution:

Solution type: Mitigation

Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connecti!

on.

Affected Software/OS:

Server with SSL/TLS.

Vulnerability Insight:

The flaw is due to cookie is not using 'secure' attribute, which

allows cookie to be passed to the server by the client over non-secure channel!

s (http) and allows attacker

to conduct session hijacking attacks.

Vulnerability Detection Method:

Details:

SSL/TLS: Missing `secure` Cookie Attribute

(OID: 1.3.6.1.4.1.25623.1.0.902661)

Version used: 2022-02-15T13:40:32Z

References:

url: https://www.owasp.org/index.php/SecureFlag

url: http://www.ietf.org/rfc/rfc2965.txt

url: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

Issue

NVT: SSL/TLS: Missing `secure` Cookie Attribute

OID: 1.3.6.1.4.1.25623.1.0.902661

Threat: Medium (CVSS: 6.4)

Port: 2087/tcp

Summary:

a server with SSL/TLS is prone to an information disclosure vulnerability.

Vulnerability Detection Result:

The cookies:

Set-Cookie: Horde=***replaced***; HttpOnly; domain=.114.154.255.43.host.securese!

rver.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087

Set-Cookie: horde_secret_key=***replaced***; HttpOnly; domain=.114.154.255.43.ho!

st.secureserver.net; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087

are missing the "secure" attribute.

Solution:

Solution type: Mitigation

Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connecti!

on.

Affected Software/OS:

Server with SSL/TLS.

Vulnerability Insight:

The flaw is due to cookie is not using 'secure' attribute, which

allows cookie to be passed to the server by the client over non-secure channel!

s (http) and allows attacker

to conduct session hijacking attacks.

Vulnerability Detection Method:

Details:

SSL/TLS: Missing `secure` Cookie Attribute

(OID: 1.3.6.1.4.1.25623.1.0.902661)

Version used: 2022-02-15T13:40:32Z

References:

url: https://www.owasp.org/index.php/SecureFlag

url: http://www.ietf.org/rfc/rfc2965.txt

url: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

Issue

NVT: Weak Host Key Algorithm(s) (SSH)

OID: 1.3.6.1.4.1.25623.1.0.117687

Threat: Medium (CVSS: 5.3)

Port: 22/tcp

Summary:

The remote SSH server is configured to allow / support weak host

key algorithm(s).

Vulnerability Detection Result:

The remote SSH server supports the following weak host key algorithm(s):

host key algorithm | Description

----------!

---

ssh-dss | Digital Signature Algorithm (DSA) / Digital Signature Stand!

ard (DSS)

Solution:

Solution type: Mitigation

Disable the reported weak host key algorithm(s).

Vulnerability Detection Method:

Checks the supported host key algorithms of the remote SSH

server.

Currently weak host key algorithms are defined as the following:

- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS!

)

Details:

Weak Host Key Algorithm(s) (SSH)

(OID: 1.3.6.1.4.1.25623.1.0.117687)

Version used: 2021-11-24T06:31:19Z

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.150713

Threat: Medium (CVSS: 5.3)

Port: 22/tcp

Summary:

The remote SSH server is configured to allow / support weak key

exchange (KEX) algorithm(s).

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

diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group!

) and 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 Dif!

fie-Hellman key

exchange. Practitioners believed this was safe as long as new key exchange mes!
sages were generated
for every connection. However, the first step in the number field sieve-the mo!
st efficient
algorithm for breaking a Diffie-Hellman connection-is dependent only on this p!
rime.
A nation-state can break a 1024-bit prime.

Vulnerability Detection Method:
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 gr!
oup / 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: 2021-11-24T06:31:19Z

References:
url: https://weakdh.org/sysadmin.html
url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html
url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.section.5
url: https://datatracker.ietf.org/doc/html/rfc6194

Issue

NVT: SSL/TLS: Report Weak Cipher Suites

OID: 1.3.6.1.4.1.25623.1.0.103440

Threat: Medium (CVSS: 5.0)

Port: 21/tcp

Summary:

This routine reports all Weak SSL/TLS cipher suites accepted

by a service.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher s!

uites on port

25/tcp is reported. If too strong cipher suites are configured for this servic!

e the alternative

would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result:

'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DH_anon_WITH_RC4_128_MD5

TLS_ECDHE_RSA_WITH_RC4_128_SHA

TLS_ECDH_anon_WITH_RC4_128_SHA

TLS_RSA_WITH_RC4_128_MD5

TLS_RSA_WITH_RC4_128_SHA

TLS_RSA_WITH_SEED_CBC_SHA

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.

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 we!

ak

- 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:

Details:

SSL/TLS: Report Weak Cipher Suites

(OID: 1.3.6.1.4.1.25623.1.0.103440)

Version used: 2021-12-01T13:10:37Z

References:

cve: CVE-2013-2566

cve: CVE-2015-2808

cve: CVE-2015-4000

url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html

url: https://bettercrypto.org/

url: https://mozilla.github.io/server-side-tls/ssl-config-generator/

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

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-2021-0775

dfn-cert: DFN-CERT-2020-1561

dfn-cert: DFN-CERT-2020-1276

dfn-cert: DFN-CERT-2017-1821

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-2015-1853

dfn-cert: DFN-CERT-2015-1679

dfn-cert: DFN-CERT-2015-1632

dfn-cert: DFN-CERT-2015-1608

dfn-cert: DFN-CERT-2015-1542

dfn-cert: DFN-CERT-2015-1518

dfn-cert: DFN-CERT-2015-1406

dfn-cert: DFN-CERT-2015-1341

dfn-cert: DFN-CERT-2015-1194

dfn-cert: DFN-CERT-2015-1144

dfn-cert: DFN-CERT-2015-1113

dfn-cert: DFN-CERT-2015-1078

dfn-cert: DFN-CERT-2015-1067

dfn-cert: DFN-CERT-2015-1038

dfn-cert: DFN-CERT-2015-1016

dfn-cert: DFN-CERT-2015-1012

dfn-cert: DFN-CERT-2015-0980

dfn-cert: DFN-CERT-2015-0977

dfn-cert: DFN-CERT-2015-0976

dfn-cert: DFN-CERT-2015-0960

dfn-cert: DFN-CERT-2015-0956

dfn-cert: DFN-CERT-2015-0944

dfn-cert: DFN-CERT-2015-0937

dfn-cert: DFN-CERT-2015-0925

dfn-cert: DFN-CERT-2015-0884

dfn-cert: DFN-CERT-2015-0881

dfn-cert: DFN-CERT-2015-0879

dfn-cert: DFN-CERT-2015-0866

dfn-cert: DFN-CERT-2015-0844

dfn-cert: DFN-CERT-2015-0800

dfn-cert: DFN-CERT-2015-0737

dfn-cert: DFN-CERT-2015-0696

dfn-cert: DFN-CERT-2014-0977

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117761

Threat: Medium (CVSS: 5.0)

Port: 110/tcp

Summary:

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

vulnerability.

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 connec!

tion.

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 protoc!

ols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security S!

ervices (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, n!

ot a security

library, to prevent or limit renegotiation when it is inappropriate within a s!

pecific 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 conne!

ction.

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: 2021-11-15T10:28:20Z

References:

cve: CVE-2011-1473

cve: CVE-2011-5094

url: https://orchilles.com/ssl-renegotiation-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

url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation

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-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

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117761

Threat: Medium (CVSS: 5.0)

Port: 143/tcp

Summary:

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

vulnerability.

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 connec!

tion.

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 protoc!

ols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security S!
ervices (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, n!
ot a security
library, to prevent or limit renegotiation when it is inappropriate within a s!
pecific 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 conne!
ction.
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: 2021-11-15T10:28:20Z

References:
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://orchilles.com/ssl-renegotiation-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

url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation

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-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

Issue

NVT: FTP Unencrypted Cleartext Login

OID: 1.3.6.1.4.1.25623.1.0.108528

Threat: Medium (CVSS: 4.8)

Port: 21/tcp

Summary:

The remote host is running a FTP service that allows cleartext logins over

unencrypted connections.

Vulnerability Detection Result:

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command!

. Response(s):

Non-anonymous sessions: 331 User openvasvt OK. Password required

Anonymous sessions: 331 User anonymous OK. Password required

The remote FTP service supports the 'AUTH TLS' command but isn't enforcing the u!

se of it for:

- Non-anonymous sessions

- Anonymous sessions

Impact:

An attacker can uncover login names and passwords by sniffing traffic to the

FTP service.

Solution:

Solution type: Mitigation

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see

the manual of the FTP service for more information.

Vulnerability Detection Method:

Tries to login to a non FTPS enabled FTP service without sending a

'AUTH TLS' command first and checks if the service is accepting the login with!

out enforcing the use of

the 'AUTH TLS' command.

Details:

FTP Unencrypted Cleartext Login

(OID: 1.3.6.1.4.1.25623.1.0.108528)

Version used: 2020-08-24T08:40:10Z

Issue

NVT: IMAP Unencrypted Cleartext Login

OID: 1.3.6.1.4.1.25623.1.0.15856

Threat: Medium (CVSS: 4.8)

Port: 143/tcp

Summary:

The remote host is running an IMAP daemon that allows cleartext logins over

unencrypted connections.

NOTE: Valid credentials needs to given to the settings of 'Login configuration!

s' OID: 1.3.6.1.4.1.25623.1.0.10870.

Vulnerability Detection Result:

The remote IMAP server accepts logins via the following cleartext authentication!

mechanisms over unencrypted connections:

AUTH=LOGIN

AUTH=PLAIN

The remote IMAP server supports the 'STARTTLS' command but isn't enforcing the u!

se of it for the cleartext authentication mechanisms.

Impact:

An attacker can uncover user names and passwords by sniffing traffic to the IMAP

daemon if a less secure authentication mechanism (eg, LOGIN command, AUTH=PLAI!

N, AUTH=LOGIN) is used.

Solution:

Solution type: Mitigation

Configure the remote server to always enforce encrypted connections via

SSL/TLS with the 'STARTTLS' command.

Vulnerability Detection Method:

Details:

IMAP Unencrypted Cleartext Login

(OID: 1.3.6.1.4.1.25623.1.0.15856)

Version used: 2020-08-24T15:18:35Z

References:

osvdb: 3119

url: http://www.ietf.org/rfc/rfc2222.txt

url: http://www.ietf.org/rfc/rfc2595.txt

Issue

NVT: POP3 Unencrypted Cleartext Login

OID: 1.3.6.1.4.1.25623.1.0.15855

Threat: Medium (CVSS: 4.8)

Port: 110/tcp

Summary:

The remote host is running a POP3 daemon that allows cleartext logins over

unencrypted connections.

NOTE: Depending on the POP3 server configuration valid credentials needs to be!

given to the settings of

'Login configurations' OID: 1.3.6.1.4.1.25623.1.0.10870.

Vulnerability Detection Result:

The remote POP3 server accepts logins via the following cleartext authentication!

mechanisms over unencrypted connections:

USER

SASL PLAIN LOGIN

The remote POP3 server supports the 'STLS' command but isn't enforcing the use o!

f it for the cleartext authentication mechanisms.

Impact:

An attacker can uncover user names and passwords by sniffing traffic to the POP3

daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN!

, AUTH LOGIN) is used.

Solution:

Solution type: Mitigation

Configure the remote server to always enforce encrypted connections via

SSL/TLS with the 'STLS' command.

Vulnerability Detection Method:

Details:

POP3 Unencrypted Cleartext Login

(OID: 1.3.6.1.4.1.25623.1.0.15855)

Version used: 2020-08-24T15:18:35Z

References:

osvdb: 3119

url: http://www.ietf.org/rfc/rfc2222.txt

url: http://www.ietf.org/rfc/rfc2595.txt

Issue

NVT: SMTP Unencrypted Cleartext Login

OID: 1.3.6.1.4.1.25623.1.0.108530

Threat: Medium (CVSS: 4.8)

Port: 587/tcp

Summary:

The remote host is running a SMTP server that allows cleartext logins over

unencrypted connections.

Vulnerability Detection Result:

The remote SMTP server accepts logins via the following cleartext authentication!

mechanisms over unencrypted connections:

PLAIN

LOGIN

The remote SMTP server supports the 'STARTTLS' command but isn't enforcing the u!

se of it for the cleartext authentication mechanisms.

Impact:

An attacker can uncover login names and passwords by sniffing traffic to the

SMTP server.

Solution:

Solution type: Mitigation

Enable SMTPS or enforce the connection via the 'STARTTLS' command. Please see

the manual of the SMTP server for more information.

Vulnerability Detection Method:

Evaluates from previously collected info if a non SMTPS enabled SMTP server

is providing the 'PLAIN' or 'LOGIN' authentication methods without sending the!

'STARTTLS' command first.

Details:

SMTP Unencrypted Cleartext Login

(OID: 1.3.6.1.4.1.25623.1.0.108530)

Version used: 2020-08-24T15:18:35Z

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117274

Threat: Medium (CVSS: 4.3)

Port: 2087/tcp

Summary:

It was possible to detect the usage of the deprecated TLSv1.0

and/or TLSv1.1 protocol on this system.

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 can!

be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256!

23.1.0.802067) 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 s!

ensitive data

transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive se!
curity 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 reference!
s 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 Downgra!
ded 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: 2021-07-19T08:11:48Z

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: 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

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117274

Threat: Medium (CVSS: 4.3)

Port: 2096/tcp

Summary:

It was possible to detect the usage of the deprecated TLSv1.0

and/or TLSv1.1 protocol on this system.

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 can!

be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256!

23.1.0.802067) 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 s!

ensitive data

transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive se!

curity 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 reference!

s 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 Downgra!

ded 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: 2021-07-19T08:11:48Z

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: 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

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117274

Threat: Medium (CVSS: 4.3)

Port: 993/tcp

Summary:

It was possible to detect the usage of the deprecated TLSv1.0

and/or TLSv1.1 protocol on this system.

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 can!

be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256!

23.1.0.802067) 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 s!

ensitive data

transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive se!

curity 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 reference!

s 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 Downgra!

ded 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: 2021-07-19T08:11:48Z

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: 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

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117274

Threat: Medium (CVSS: 4.3)

Port: 995/tcp

Summary:

It was possible to detect the usage of the deprecated TLSv1.0

and/or TLSv1.1 protocol on this system.

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 can!

be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256!

23.1.0.802067) 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 s!

ensitive data

transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive se!

curity 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 reference!

s 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 Downgra!

ded 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: 2021-07-19T08:11:48Z

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: 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

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117274

Threat: Medium (CVSS: 4.3)

Port: 143/tcp

Summary:

It was possible to detect the usage of the deprecated TLSv1.0

and/or TLSv1.1 protocol on this system.

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 can!

be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256!

23.1.0.802067) 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 s!
ensitive data
transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive se!
curity 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 reference!
s 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 Downgra!
ded 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: 2021-07-19T08:11:48Z

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: 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

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117274

Threat: Medium (CVSS: 4.3)

Port: 110/tcp

Summary:

It was possible to detect the usage of the deprecated TLSv1.0

and/or TLSv1.1 protocol on this system.

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 can!

be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256!

23.1.0.802067) 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 s!

ensitive data

transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive se!

curity 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 reference!

s 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 Downgra!

ded 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: 2021-07-19T08:11:48Z

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: 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

Issue

NVT: Apache HTTP Server ETag Header Information Disclosure Weakness

OID: 1.3.6.1.4.1.25623.1.0.103122

Threat: Medium (CVSS: 4.3)

Port: 80/tcp

Product detection result: cpe:/a:apache:http_server

Detected by: Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)

Summary:

A weakness has been discovered in the Apache HTTP Server

if configured to use the FileETag directive.

Vulnerability Detection Result:

Information that was gathered:

Inode: 3014686

Size: 1963

Impact:

Exploitation of this issue may provide an attacker with

information that may be used to launch further attacks against a target networ!

k.

Solution:

Solution type: VendorFix

OpenBSD has released a patch that addresses this issue.

Inode numbers returned from the server are now encoded using a private hash to!

avoid the

release of sensitive information.

Novell has released TID10090670 to advise users to apply the available workaro!

und of

disabling the directive in the configuration file for Apache releases on NetWa!

re. Please

see the attached Technical Information Document for further details.

Vulnerability Detection Method:

Due to the way in which Apache HTTP Server generates

ETag response headers, it may be possible for an attacker to obtain sensitive !

information

regarding server files. Specifically, ETag header fields returned to a client !

contain the

file's inode number.

Details:

Apache HTTP Server ETag Header Information Disclosure Weakness

(OID: 1.3.6.1.4.1.25623.1.0.103122)

Version used: 2022-04-28T13:38:57Z

Product Detection Result:

Product:cpe:/a:apache:http_server

Method:Apache HTTP Server Detection Consolidation

(OID: 1.3.6.1.4.1.25623.1.0.117232)

References:

cve: CVE-2003-1418

url: http://www.securityfocus.com/bid/6939

url: http://httpd.apache.org/docs/mod/core.html#fileetag

url: http://www.openbsd.org/errata32.html

url: http://support.novell.com/docs/Tids/Solutions/10090670.html

cert-bund: CB-K17/1750

cert-bund: CB-K17/0896

cert-bund: CB-K15/0469

dfn-cert: DFN-CERT-2017-1821

dfn-cert: DFN-CERT-2017-0925

dfn-cert: DFN-CERT-2015-0495

Issue

NVT: Apache HTTP Server ETag Header Information Disclosure Weakness

OID: 1.3.6.1.4.1.25623.1.0.103122

Threat: Medium (CVSS: 4.3)

Port: 443/tcp

Product detection result: cpe:/a:apache:http_server

Detected by: Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)

Summary:

A weakness has been discovered in the Apache HTTP Server

if configured to use the FileETag directive.

Vulnerability Detection Result:

Information that was gathered:

Inode: 3014686

Size: 1963

Impact:

Exploitation of this issue may provide an attacker with

information that may be used to launch further attacks against a target networ!

k.

Solution:

Solution type: VendorFix

OpenBSD has released a patch that addresses this issue.

Inode numbers returned from the server are now encoded using a private hash to!

avoid the

release of sensitive information.

Novell has released TID10090670 to advise users to apply the available workaro!

und of

disabling the directive in the configuration file for Apache releases on NetWa!

re. Please

see the attached Technical Information Document for further details.

Vulnerability Detection Method:

Due to the way in which Apache HTTP Server generates

ETag response headers, it may be possible for an attacker to obtain sensitive !

information

regarding server files. Specifically, ETag header fields returned to a client !

contain the

file's inode number.

Details:

Apache HTTP Server ETag Header Information Disclosure Weakness

(OID: 1.3.6.1.4.1.25623.1.0.103122)

Version used: 2022-04-28T13:38:57Z

Product Detection Result:

Product:cpe:/a:apache:http_server

Method:Apache HTTP Server Detection Consolidation

(OID: 1.3.6.1.4.1.25623.1.0.117232)

References:

cve: CVE-2003-1418

url: http://www.securityfocus.com/bid/6939

url: http://httpd.apache.org/docs/mod/core.html#fileetag

url: http://www.openbsd.org/errata32.html

url: http://support.novell.com/docs/Tids/Solutions/10090670.html

cert-bund: CB-K17/1750

cert-bund: CB-K17/0896

cert-bund: CB-K15/0469

dfn-cert: DFN-CERT-2017-1821

dfn-cert: DFN-CERT-2017-0925

dfn-cert: DFN-CERT-2015-0495

Issue

NVT: Weak Encryption Algorithm(s) Supported (SSH)

OID: 1.3.6.1.4.1.25623.1.0.105611

Threat: Medium (CVSS: 4.3)

Port: 22/tcp

Summary:

The remote SSH server is configured to allow / support weak

encryption algorithm(s).

Vulnerability Detection Result:

The remote SSH server supports the following weak client-to-server encryption al!

gorithm(s):

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

The remote SSH server supports the following weak server-to-client encryption al!

gorithm(s):

3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

Solution:

Solution type: Mitigation

Disable the reported weak encryption algorithm(s).

Vulnerability Insight:

- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit

keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCH!

NEIER]. Arcfour

(and RC4) has problems with weak keys, and should not be used anymore.

- The 'none' algorithm specifies that no encryption is to be done. Note that t!

his method provides

no confidentiality protection, and it is NOT RECOMMENDED to use it.

- A vulnerability exists in SSH messages that employ CBC mode that may allow a!

n attacker to

recover plaintext from a block of ciphertext.

Vulnerability Detection Method:

Checks the supported encryption algorithms (client-to-server

and server-to-client) of the remote SSH server.

Currently weak encryption algorithms are defined as the following:

- Arcfour (RC4) cipher based algorithms

- none algorithm

- CBC mode cipher based algorithms

Details:

Weak Encryption Algorithm(s) Supported (SSH)

(OID: 1.3.6.1.4.1.25623.1.0.105611)

Version used: 2021-09-20T08:25:27Z

References:

url: https://tools.ietf.org/html/rfc4253#section-6.3

url: https://www.kb.cert.org/vuls/id/958563

Issue

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

OID: 1.3.6.1.4.1.25623.1.0.117274

Threat: Medium (CVSS: 4.3)

Port: 2078/tcp

Summary:

It was possible to detect the usage of the deprecated TLSv1.0

and/or TLSv1.1 protocol on this system.

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 can!
be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.256!
23.1.0.802067) 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 s!
ensitive data
transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive se!
curity 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 reference!
s 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 Downgra!

ded 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: 2021-07-19T08:11:48Z

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: 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

Issue

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.106223

Threat: Medium (CVSS: 4.0)

Port: 110/tcp

Summary:

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength

(key size < 2048).

Vulnerability Detection Result:

Server Temporary Key Size: 1024 bits

Impact:

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use

a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers:

Beginning with version 2.4.7, mod_ssl will use DH parameters which include pri!

mes with lengths of more than 1024 bits.

Vulnerability Insight:

The Diffie-Hellman group are some big numbers that are used as base for

the DH computations. They can be, and often are, fixed. The security of the fi!

nal secret depends on the size

of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits !

to be breakable by really

powerful attackers like governments.

Vulnerability Detection Method:

Checks the DHE temporary public key size.

Details:

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerab...

(OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: 2021-02-12T06:42:15Z

References:

url: https://weakdh.org/

url: https://weakdh.org/sysadmin.html

Issue

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.106223

Threat: Medium (CVSS: 4.0)

Port: 143/tcp

Summary:

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength

(key size < 2048).

Vulnerability Detection Result:

Server Temporary Key Size: 1024 bits

Impact:

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use

a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers:

Beginning with version 2.4.7, mod_ssl will use DH parameters which include pri!

mes with lengths of more than 1024 bits.

Vulnerability Insight:

The Diffie-Hellman group are some big numbers that are used as base for

the DH computations. They can be, and often are, fixed. The security of the fi!

nal secret depends on the size

of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits !

to be breakable by really

powerful attackers like governments.

Vulnerability Detection Method:

Checks the DHE temporary public key size.

Details:

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerab...

(OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: 2021-02-12T06:42:15Z

References:

url: https://weakdh.org/

url: https://weakdh.org/sysadmin.html

Issue

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.106223

Threat: Medium (CVSS: 4.0)

Port: 993/tcp

Summary:

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength

(key size < 2048).

Vulnerability Detection Result:

Server Temporary Key Size: 1024 bits

Impact:

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use

a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers:

Beginning with version 2.4.7, mod_ssl will use DH parameters which include pri!

mes with lengths of more than 1024 bits.

Vulnerability Insight:

The Diffie-Hellman group are some big numbers that are used as base for

the DH computations. They can be, and often are, fixed. The security of the fi!

nal secret depends on the size

of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits !

to be breakable by really

powerful attackers like governments.

Vulnerability Detection Method:

Checks the DHE temporary public key size.

Details:

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerab...

(OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: 2021-02-12T06:42:15Z

References:

url: https://weakdh.org/

url: https://weakdh.org/sysadmin.html

Issue

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

OID: 1.3.6.1.4.1.25623.1.0.106223

Threat: Medium (CVSS: 4.0)

Port: 995/tcp

Summary:

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength

(key size < 2048).

Vulnerability Detection Result:

Server Temporary Key Size: 1024 bits

Impact:

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution:

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use

a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers:

Beginning with version 2.4.7, mod_ssl will use DH parameters which include pri!

mes with lengths of more than 1024 bits.

Vulnerability Insight:

The Diffie-Hellman group are some big numbers that are used as base for

the DH computations. They can be, and often are, fixed. The security of the fi!

nal secret depends on the size

of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits !

to be breakable by really

powerful attackers like governments.

Vulnerability Detection Method:

Checks the DHE temporary public key size.

Details:

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerab...

(OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: 2021-02-12T06:42:15Z

References:

url: https://weakdh.org/

url: https://weakdh.org/sysadmin.html

Issue

NVT: Weak MAC Algorithm(s) Supported (SSH)

OID: 1.3.6.1.4.1.25623.1.0.105610

Threat: Low (CVSS: 2.6)

Port: 22/tcp

Summary:

The remote SSH server is configured to allow / support weak MAC

algorithm(s).

Vulnerability Detection Result:

The remote SSH server supports the following weak client-to-server MAC algorithm!

(s):

hmac-md5

hmac-md5-96

hmac-sha1-96

The remote SSH server supports the following weak server-to-client MAC algorithm!

(s):

hmac-md5

hmac-md5-96

hmac-sha1-96

Solution:

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method:

Checks the supported MAC algorithms (client-to-server and

server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms

- 96-bit based algorithms

- none algorithm

Details:

Weak MAC Algorithm(s) Supported (SSH)

(OID: 1.3.6.1.4.1.25623.1.0.105610)

Version used: 2021-09-20T11:05:40Z