Scan Report

March 10, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Scan Porto”. The scan started at Fri Mar 10 03:25:39 2023 UTC and ended at Fri Mar 10 03:52:42 2023 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
192.168.60.2	4	10	2	0	0
192.168.60.3 ubuntuserver	0	6	2	0	0
192.168.60.1	0	1	1	0	0
192.168.60.7	0	1	0	0	0
192.168.60.10	0	0	2	0	0
192.168.60.254 router.citeforma.pt	0	0	2	0	0
192.168.60.4	0	0	1	0	0
Total: 7	4	18	10	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 32 results selected by the filtering described above. Before filtering there were 209 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.60.2	SSH	Failure	Protocol SSH, Port 22006, User root : Login failure
192.168.60.3 - ubuntuserver	SSH	Failure	Protocol SSH, Port 22006, User root : Login failure
192.168.60.1	SSH	Failure	Protocol SSH, Port 22006, User root : Login failure
192.168.60.7	SSH	Failure	Protocol SSH, Port 22006, User root : Login failure
192.168.60.10	SSH	Failure	Protocol SSH, Port 22006, User root : Login failure
192.168.60.4	SSH	Failure	Protocol SSH, Port 22006, User root : Login failure

2 Results per Host

2.1 192.168.60.2

Host scan start	Fri Mar 10 03:26:12 2023 UTC
Host scan end	Fri Mar 10 03:36:51 2023 UTC

Service (Port)	Threat Level
8889/tcp	High
8888/tcp	High
8889/tcp	Medium
8888/tcp	Medium
general/tcp	Low
general/icmp	Low

2.1.1 High 8889/tcp

High (CVSS: 10.0)
NVT: Openfire < 4.5.5, 4.6.x < 4.6.6 Multiple Log4j Vulnerabilities (Log4Shell)

Summary
Openfire is prone to multiple vulnerabilities in the Apache Log4j library.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.5.5
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 4.5.5, 4.6.6 or later.

Affected Software/OS
Openfire prior to version 4.5.5 and 4.6.x prior to 4.6.6.

Vulnerability Insight
The following vulnerabilities exist:
CVE-2021-44228: Apache Log4j2 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. This vulnerability is dubbed 'Log4Shell'.
CVE-2021-45046: Denial of Service (DoS) and a possible remote code execution (RCE) in certain non-default configurations.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire < 4.5.5, 4.6.x < 4.6.6 Multiple Log4j Vulnerabilities (Log4Shell)`
OID:1.3.6.1.4.1.25623.1.0.147315
Version used: `2022-08-09T10:11:17Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2021-44228
cve: CVE-2021-45046
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://discourse.igniterealtime.org/t/openfire-4-6-6-and-4-5-5-releases-lo
↪g4j-only-changes/91139
url: https://github.com/advisories/GHSA-jfh8-c2jp-5v3q
url: https://www.openwall.com/lists/oss-security/2021/12/10/1
url: https://www.lunasec.io/docs/blog/log4j-zero-day/
url: https://www.lunasec.io/docs/blog/log4j-zero-day-update-on-cve-2021-45046/
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1175
cert-bund: WID-SEC-2022-1015
cert-bund: WID-SEC-2022-0352
cert-bund: WID-SEC-2022-0351
cert-bund: CB-K22/0285
cert-bund: CB-K22/0148
cert-bund: CB-K22/0029
cert-bund: CB-K21/1283
cert-bund: CB-K21/1264
dfn-cert: DFN-CERT-2022-1813
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0591
dfn-cert: DFN-CERT-2022-0153
dfn-cert: DFN-CERT-2022-0146
dfn-cert: DFN-CERT-2022-0096
dfn-cert: DFN-CERT-2022-0081
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2022-0008
dfn-cert: DFN-CERT-2021-2666
dfn-cert: DFN-CERT-2021-2634
dfn-cert: DFN-CERT-2021-2633
dfn-cert: DFN-CERT-2021-2624
dfn-cert: DFN-CERT-2021-2623
dfn-cert: DFN-CERT-2021-2620
dfn-cert: DFN-CERT-2021-2619
dfn-cert: DFN-CERT-2021-2616
dfn-cert: DFN-CERT-2021-2598
dfn-cert: DFN-CERT-2021-2588
dfn-cert: DFN-CERT-2021-2585
dfn-cert: DFN-CERT-2021-2582
dfn-cert: DFN-CERT-2021-2581
dfn-cert: DFN-CERT-2021-2576
```

High (CVSS: 9.8)
NVT: Openfire < 4.4.3 Multiple Vulnerabilities

Summary
Openfire is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.4.3
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 4.4.3 or later.

Affected Software/OS
Openfire version 4.4.2 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- Directory traversal (CVE-2019-18393)
- Server Side Request Forgery (SSRF) (CVE-2019-18394)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire < 4.4.3 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.144353
Version used: `2021-07-13T02:01:14Z`

References

```
cve: CVE-2019-18393
cve: CVE-2019-18394
url: https://swarm.ptsecurity.com/openfire-admin-console/
url: https://github.com/igniterealtime/Openfire/pull/1498
url: https://github.com/igniterealtime/Openfire/pull/1497
```

[return to 192.168.60.2]

2.1.2 High 8888/tcp

High (CVSS: 10.0)
NVT: Openfire < 4.5.5, 4.6.x < 4.6.6 Multiple Log4j Vulnerabilities (Log4Shell)

Summary

. . . continues on next page . . .

... continued from previous page ...

Openfire is prone to multiple vulnerabilities in the Apache Log4j library.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.5.5
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 4.5.5, 4.6.6 or later.

Affected Software/OS
Openfire prior to version 4.5.5 and 4.6.x prior to 4.6.6.

Vulnerability Insight
The following vulnerabilities exist:
CVE-2021-44228: Apache Log4j2 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. This vulnerability is dubbed 'Log4Shell'.
CVE-2021-45046: Denial of Service (DoS) and a possible remote code execution (RCE) in certain non-default configurations.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire < 4.5.5, 4.6.x < 4.6.6 Multiple Log4j Vulnerabilities (Log4Shell)`
OID:1.3.6.1.4.1.25623.1.0.147315
Version used: `2022-08-09T10:11:17Z`

References

```
cve: CVE-2021-44228
cve: CVE-2021-45046
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://discourse.igniterealtime.org/t/openfire-4-6-6-and-4-5-5-releases-lo
↪g4j-only-changes/91139
url: https://github.com/advisories/GHSA-jfh8-c2jp-5v3q
url: https://www.openwall.com/lists/oss-security/2021/12/10/1
url: https://www.lunasec.io/docs/blog/log4j-zero-day/
url: https://www.lunasec.io/docs/blog/log4j-zero-day-update-on-cve-2021-45046/
cert-bund: WID-SEC-2023-0063
cert-bund: WID-SEC-2022-1175
cert-bund: WID-SEC-2022-1015
cert-bund: WID-SEC-2022-0352
```

... continues on next page ...

. . . continued from previous page . . .

```
cert-bund: WID-SEC-2022-0351
cert-bund: CB-K22/0285
cert-bund: CB-K22/0148
cert-bund: CB-K22/0029
cert-bund: CB-K21/1283
cert-bund: CB-K21/1264
dfn-cert: DFN-CERT-2022-1813
dfn-cert: DFN-CERT-2022-0805
dfn-cert: DFN-CERT-2022-0591
dfn-cert: DFN-CERT-2022-0153
dfn-cert: DFN-CERT-2022-0146
dfn-cert: DFN-CERT-2022-0096
dfn-cert: DFN-CERT-2022-0081
dfn-cert: DFN-CERT-2022-0074
dfn-cert: DFN-CERT-2022-0068
dfn-cert: DFN-CERT-2022-0008
dfn-cert: DFN-CERT-2021-2666
dfn-cert: DFN-CERT-2021-2634
dfn-cert: DFN-CERT-2021-2633
dfn-cert: DFN-CERT-2021-2624
dfn-cert: DFN-CERT-2021-2623
dfn-cert: DFN-CERT-2021-2620
dfn-cert: DFN-CERT-2021-2619
dfn-cert: DFN-CERT-2021-2616
dfn-cert: DFN-CERT-2021-2598
dfn-cert: DFN-CERT-2021-2588
dfn-cert: DFN-CERT-2021-2585
dfn-cert: DFN-CERT-2021-2582
dfn-cert: DFN-CERT-2021-2581
dfn-cert: DFN-CERT-2021-2576
```

High (CVSS: 9.8)
NVT: Openfire < 4.4.3 Multiple Vulnerabilities

Summary
Openfire is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.4.3
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 4.4.3 or later.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
Openfire version 4.4.2 and prior.

Vulnerability Insight
The following vulnerabilities exist:
- Directory traversal (CVE-2019-18393)
- Server Side Request Forgery (SSRF) (CVE-2019-18394)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire < 4.4.3 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.144353
Version used: `2021-07-13T02:01:14Z`

References
```
cve: CVE-2019-18393
cve: CVE-2019-18394
url: https://swarm.ptsecurity.com/openfire-admin-console/
url: https://github.com/igniterealtime/Openfire/pull/1498
url: https://github.com/igniterealtime/Openfire/pull/1497
```

[return to 192.168.60.2]

2.1.3 Medium 8889/tcp

Medium (CVSS: 6.1)
NVT: Openfire 4.3.x < 4.5.0 Multiple XSS Vulnerabilities

Summary
Openfire is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.3.2
Fixed version:     4.5.0
Installation
path / port:       /
```

Impact
Successful exploitation would allow a remote attacker to inject arbitrary script commands into the affected application.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to version 4.5.0 to fix the issue.

Affected Software/OS
Openfire 4.3.x through 4.4.x.

Vulnerability Insight
The flaws exist in various parameters of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire 4.3.x < 4.5.0 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.112684
Version used: `2021-07-13T02:01:14Z`

References

```
cve: CVE-2019-20363
cve: CVE-2019-20364
cve: CVE-2019-20365
cve: CVE-2019-20366
url: https://issues.igniterealtime.org/browse/OF-1955
url: https://github.com/igniterealtime/Openfire/pull/1561
```

Medium (CVSS: 6.1)
NVT: Openfire < 4.5.2 Multiple Vulnerabilities

Summary
Openfire is prone to multiple cross-site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.5.2
Installation
path / port:       /
```

Solution:
Solution type: VendorFix
Update to version 4.5.2 or later.

Affected Software/OS
Openfire version 4.5.1 and probably prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire < 4.5.2 Multiple Vulnerabilities`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.144532
Version used: `2021-07-13T02:01:14Z`

References

```
cve: CVE-2020-24601
cve: CVE-2020-24602
cve: CVE-2020-24604
url: https://issues.igniterealtime.org/browse/OF-1963
```

Medium (CVSS: 6.1)
NVT: Openfire <= 4.6.4 Multiple XSS Vulnerabilities

Summary
Openfire is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     None
Installation
path / port:       /
```

Impact
Successful exploitation would allow a remote attacker to inject arbitrary script commands into the affected application.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
Openfire version 4.6.4 and probably prior.

Vulnerability Insight
The flaws exist in various parameters of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire <= 4.6.4 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.145064
Version used: `2021-12-22T14:23:41Z`

References

```
cve: CVE-2020-35127
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2020-35199
cve: CVE-2020-35200
cve: CVE-2020-35201
cve: CVE-2020-35202
url: https://discourse.igniterealtime.org/t/openfire-4-6-0-has-stored-xss-vulner
↪abilities/89276
url: https://www.exploit-db.com/exploits/49233
url: https://discourse.igniterealtime.org/t/openfire-4-6-0-has-reflective-xss-vu
↪lnerabilities/89296
url: https://www.exploit-db.com/exploits/49234
url: https://www.exploit-db.com/exploits/49235
```

Medium (CVSS: 6.1)
NVT: Openfire < 4.4.2 Multiple Vulnerabilities

Summary
Openfire is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.4.2
Installation
path / port:       /
```

Impact
Successful exploitation would allow a remote attacker to inject arbitrary script commands into the affected application, disclose information or write arbitrary files on the system, typically resulting in remote command execution.

Solution:
Solution type: VendorFix
Update to version 4.4.2 to fix the issues.

Affected Software/OS
Openfire up to and includiong version 4.4.1.

Vulnerability Insight
The following issues exist and have been dealt with:
- XSS via various parameters in the setup/setup-datasource-standard.jsp (CVE-2019-20525, CVE-2019-20526, CVE-2019-20527, CVE-2019-20528)
- Admin Console - Plugin Upload vulnerable to ZipSlip (OF-1860)
- LDAP password disclosed on admin page (OF-1873)
- XSS on LDAP Server Settings page (OF-1874)

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Openfire < 4.4.2 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.112713
Version used: `2021-07-13T02:01:14Z`

References

```
cve: CVE-2019-20528
cve: CVE-2019-20525
cve: CVE-2019-20526
cve: CVE-2019-20527
url: https://www.netsparker.com/web-applications-advisories/ns-19-015-reflected-
↪cross-site-scripting-in-openfire/
url: https://issues.igniterealtime.org/browse/OF-1860
url: https://issues.igniterealtime.org/browse/OF-1873
url: https://issues.igniterealtime.org/browse/OF-1874
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

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 primes 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 final 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 Vulnerabili.`
`↪..`

. . . continues on next page . . .

. . . continued from previous page . . .

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
```

[return to 192.168.60.2]

2.1.4 Medium 8888/tcp

Medium (CVSS: 6.1)
NVT: Openfire < 4.4.2 Multiple Vulnerabilities

Summary
Openfire is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.4.2
Installation
path / port:       /
```

Impact
Successful exploitation would allow a remote attacker to inject arbitrary script commands into the affected application, disclose information or write arbitrary files on the system, typically resulting in remote command execution.

Solution:
Solution type: VendorFix
Update to version 4.4.2 to fix the issues.

Affected Software/OS
Openfire up to and includiong version 4.4.1.

Vulnerability Insight
The following issues exist and have been dealt with:
- XSS via various parameters in the setup/setup-datasource-standard.jsp (CVE-2019-20525, CVE-2019-20526, CVE-2019-20527, CVE-2019-20528)
- Admin Console - Plugin Upload vulnerable to ZipSlip (OF-1860)
- LDAP password disclosed on admin page (OF-1873)
- XSS on LDAP Server Settings page (OF-1874)

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Checks if a vulnerable version is present on the target host.
Details: `Openfire < 4.4.2 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.112713
Version used: `2021-07-13T02:01:14Z`

References

```
cve: CVE-2019-20528
cve: CVE-2019-20525
cve: CVE-2019-20526
cve: CVE-2019-20527
url: https://www.netsparker.com/web-applications-advisories/ns-19-015-reflected-
↪cross-site-scripting-in-openfire/
url: https://issues.igniterealtime.org/browse/OF-1860
url: https://issues.igniterealtime.org/browse/OF-1873
url: https://issues.igniterealtime.org/browse/OF-1874
```

Medium (CVSS: 6.1)
NVT: Openfire 4.3.x < 4.5.0 Multiple XSS Vulnerabilities

Summary
Openfire is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.5.0
Installation
path / port:       /
```

Impact
Successful exploitation would allow a remote attacker to inject arbitrary script commands into the affected application.

Solution:
Solution type: VendorFix
Update to version 4.5.0 to fix the issue.

Affected Software/OS
Openfire 4.3.x through 4.4.x.

Vulnerability Insight
The flaws exist in various parameters of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire 4.3.x < 4.5.0 Multiple XSS Vulnerabilities`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.112684
Version used: `2021-07-13T02:01:14Z`

References

```
cve: CVE-2019-20363
cve: CVE-2019-20364
cve: CVE-2019-20365
cve: CVE-2019-20366
url: https://issues.igniterealtime.org/browse/OF-1955
url: https://github.com/igniterealtime/Openfire/pull/1561
```

Medium (CVSS: 6.1)
NVT: Openfire < 4.5.2 Multiple Vulnerabilities

Summary

Openfire is prone to multiple cross-site scripting vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     4.5.2
Installation
path / port:       /
```

Solution:

Solution type: VendorFix

Update to version 4.5.2 or later.

Affected Software/OS

Openfire version 4.5.1 and probably prior.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Openfire < 4.5.2 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.144532
Version used: `2021-07-13T02:01:14Z`

References

```
cve: CVE-2020-24601
cve: CVE-2020-24602
cve: CVE-2020-24604
url: https://issues.igniterealtime.org/browse/OF-1963
```

Medium (CVSS: 6.1)
NVT: Openfire <= 4.6.4 Multiple XSS Vulnerabilities

Summary
Openfire is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.3.2
Fixed version:     None
Installation
path / port:       /
```

Impact
Successful exploitation would allow a remote attacker to inject arbitrary script commands into the affected application.

Solution:
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS
Openfire version 4.6.4 and probably prior.

Vulnerability Insight
The flaws exist in various parameters of the application.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Openfire <= 4.6.4 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.145064
Version used: `2021-12-22T14:23:41Z`

References

```
cve: CVE-2020-35127
cve: CVE-2020-35199
cve: CVE-2020-35200
cve: CVE-2020-35201
cve: CVE-2020-35202
url: https://discourse.igniterealtime.org/t/openfire-4-6-0-has-stored-xss-vulner
↪abilities/89276
url: https://www.exploit-db.com/exploits/49233
url: https://discourse.igniterealtime.org/t/openfire-4-6-0-has-reflective-xss-vu
↪lnerabilities/89296
url: https://www.exploit-db.com/exploits/49234
url: https://www.exploit-db.com/exploits/49235
```

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.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Ffckeditor%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Ffocalboard%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Ffocalboard%2Fapi%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Ffocalboard%2Fapi%2Fv2%2F:pas
↪sword
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Fplaybooks%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Fplaybooks%2Fapi%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Fplaybooks%2Fapi%2Fv0%2F:pass
↪word
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Fplaybooks%2Fapi%2Fv0%2Fplayb
↪ooks%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Fplaybooks%2Fapi%2Fv0%2Fruns%
↪2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Fservlet%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Fservlet%2Foauth%2F:password
http://192.168.60.2:8888/login.jsp?url=%2Fplugins%2Fservlet%2Foauth%2Fusers%2F:p
↪assword
```

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:

. . . continues on next page . . .

. . . continued from previous page . . .

- 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: `2020-08-24T15:18:35Z`

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 192.168.60.2]

2.1.5 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

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: 2607436120
Packet 2: 2607437196
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

References

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 192.168.60.2]

2.1.6 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

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. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2022-11-18T10:11:40Z

References

```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.60.2]

2.2 192.168.60.3

Host scan start Fri Mar 10 03:26:15 2023 UTC
Host scan end Fri Mar 10 03:39:13 2023 UTC

Service (Port)	Threat Level
25/tcp	Medium
993/tcp	Medium
143/tcp	Medium
general/tcp	Low
general/icmp	Low

2.2.1 Medium 25/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

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 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.

. . . continues on next page . . .

. . . continued from previous page . . .

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 192.168.60.3]

2.2.2 Medium 993/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=Automatically-generated IMAP SSL key,O=Courier Mail Serv
↪er,L=New York,ST=NY,C=US
Certificate details:
fingerprint (SHA-1)             | 59E077B19372B11179E21F58C77C0F9FBD80624F
fingerprint (SHA-256)           | 70202747B704048870B22641DA3DF654FBCFD14499FB29
↪3B560A52C22BF6E700
issued by                       | CN=localhost,OU=Automatically-generated IMAP S
↪SL key,O=Courier Mail Server,L=New York,ST=NY,C=US
public key algorithm            | RSA
public key size (bits)          | 3072
serial                          | 01
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=Automatically-generated IMAP S
↪SL key,O=Courier Mail Server,L=New York,ST=NY,C=US
subject alternative names (SAN) | None
valid from                      | 2023-03-05 23:54:58 UTC
valid until                     | 2024-03-04 23:54:58 UTC
```

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate with one signed by a trusted CA.

Vulnerability Detection Method
The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.
Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`
OID:1.3.6.1.4.1.25623.1.0.113054
Version used: `2021-11-22T15:32:39Z`

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

. . . 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.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

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

OID:1.3.6.1.4.1.25623.1.0.117274

Version used: `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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪-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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 192.168.60.3]

2.2.3 Medium 143/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection

Summary
The service is using an SSL/TLS certificate from a known untrusted and/or dangerous certificate authority (CA).

Vulnerability Detection Result

```
The certificate of the remote service is signed by the following untrusted and/o
↪r dangerous CA:
Issuer: CN=localhost,OU=Automatically-generated IMAP SSL key,O=Courier Mail Serv
↪er,L=New York,ST=NY,C=US
Certificate details:
fingerprint (SHA-1)             | 59E077B19372B11179E21F58C77C0F9FBD80624F
fingerprint (SHA-256)           | 70202747B704048870B22641DA3DF654FBCFD14499FB29
↪3B560A52C22BF6E700
issued by                       | CN=localhost,OU=Automatically-generated IMAP S
↪SL key,O=Courier Mail Server,L=New York,ST=NY,C=US
public key algorithm            | RSA
public key size (bits)          | 3072
serial                          | 01
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=localhost,OU=Automatically-generated IMAP S
↪SL key,O=Courier Mail Server,L=New York,ST=NY,C=US
subject alternative names (SAN) | None
valid from                      | 2023-03-05 23:54:58 UTC
valid until                     | 2024-03-04 23:54:58 UTC
```

Impact
An attacker could use this for man-in-the-middle (MITM) attacks, accessing sensible data and other attacks.

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate with one signed by a trusted CA.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

The script reads the certificate used by the target host and checks if it was signed by a known untrusted and/or dangerous CA.

Details: `SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection`

OID:1.3.6.1.4.1.25623.1.0.113054

Version used: `2021-11-22T15:32:39Z`

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.

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `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
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

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 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.

. . . continues on next page . . .

. . . continued from previous page . . .

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 192.168.60.3]

2.2.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

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: 631097629
Packet 2: 631098716
```

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`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

References

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 192.168.60.3]

2.2.5 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

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. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References
```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.60.3]

2.3 192.168.60.1

Host scan start	Fri Mar 10 03:26:15 2023 UTC
Host scan end	Fri Mar 10 03:41:51 2023 UTC

Service (Port)	Threat Level
135/tcp	Medium

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
general/tcp	Low

2.3.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
     Annotation: KeyIso
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
```

... continues on next page ...

. . . continued from previous page . . .

```
     Annotation: Impl friendly name
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_ip_tcp:192.168.60.1[49664]
     Annotation: MS NT Directory DRS Interface
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49665]
Port: 49666/tcp
     UUID: 3473dd4d-2e88-4006-9cba-22570909dd10, version 5
     Endpoint: ncacn_ip_tcp:192.168.60.1[49666]
     Annotation: WinHttp Auto-Proxy Service
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.60.1[49667]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49667]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_ip_tcp:192.168.60.1[49667]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49667]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49667]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.60.1[49667]
     Annotation: KeyIso
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49667]
     Annotation: Impl friendly name
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_ip_tcp:192.168.60.1[49667]
     Annotation: MS NT Directory DRS Interface
Port: 49669/tcp
     UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49669]
     Annotation: UserMgrCli
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49669]
     Annotation: Proxy Manager provider server endpoint
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49669]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49669]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49669]
     UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49669]
     Annotation: UserMgrCli
     UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49669]
     Annotation: Proxy Manager client server endpoint
     UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49669]
     Annotation: Adh APIs
Port: 49670/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_http:192.168.60.1[49670]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_http:192.168.60.1[49670]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_http:192.168.60.1[49670]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_http:192.168.60.1[49670]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_http:192.168.60.1[49670]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_http:192.168.60.1[49670]
     Annotation: KeyIso
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_http:192.168.60.1[49670]
     Annotation: MS NT Directory DRS Interface
Port: 49671/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Endpoint: ncacn_ip_tcp:192.168.60.1[49671]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49671]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49671]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49671]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49671]
Port: 49676/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.60.1[49676]
Port: 49683/tcp
     UUID: 5b821720-f63b-11d0-aad2-00c04fc324db, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49683]
     UUID: 6bffd098-a112-3610-9833-46c3f874532d, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[49683]
Port: 58690/tcp
     UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
     Endpoint: ncacn_ip_tcp:192.168.60.1[58690]
     Named pipe : dnsserver
     Win32 service or process : dns.exe
     Description : DNS Server
Port: 58706/tcp
     UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[58706]
     Annotation: Frs2 Service
Port: 62897/tcp
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[62897]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[62897]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.1[62897]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.60.1[62897]
     Annotation: KeyIso
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2022-06-03T10:17:07Z`

[return to 192.168.60.1]

2.3.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

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: 1332176
Packet 2: 1333268
```

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.

. . . continues on next page . . .

. . . continued from previous page . . .

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`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

References

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 192.168.60.1]

2.4 192.168.60.7

Host scan start Fri Mar 10 03:26:15 2023 UTC
Host scan end Fri Mar 10 03:52:39 2023 UTC

Service (Port)	Threat Level
135/tcp	Medium

2.4.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.60.7[49664]
     Annotation: RemoteAccessCheck
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.60.7[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49665]
Port: 49666/tcp
     UUID: 3473dd4d-2e88-4006-9cba-22570909dd10, version 5
     Endpoint: ncacn_ip_tcp:192.168.60.7[49666]
     Annotation: WinHttp Auto-Proxy Service
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     Annotation: IdSegSrv service
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     Annotation: Proxy Manager provider server endpoint
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     Annotation: XactSrv service
     UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     Annotation: Proxy Manager client server endpoint
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     Annotation: Adh APIs
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49667]
     Annotation: Impl friendly name
Port: 49668/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49668]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49668]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49668]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49668]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49668]
Port: 49669/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.60.7[49669]
     Annotation: RemoteAccessCheck
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49669]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.60.7[49669]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.60.7[49669]
     Annotation: KeyIso
Port: 49670/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.60.7[49670]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2022-06-03T10:17:07Z`

[return to 192.168.60.7]

2.5 192.168.60.10

Host scan start	Fri Mar 10 03:26:15 2023 UTC
Host scan end	Fri Mar 10 03:38:57 2023 UTC

Service (Port)	Threat Level
general/icmp	Low
general/tcp	Low

2.5.1 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

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. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References

```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.60.10]

2.5.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

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: 3091850686
Packet 2: 3091851777
```

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

... continues on next page ...

. . . continued from previous page . . .

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`

OID:1.3.6.1.4.1.25623.1.0.80091

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

References

```
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
```

[return to 192.168.60.10]

2.6 192.168.60.254

Host scan start	Fri Mar 10 03:26:15 2023 UTC
Host scan end	Fri Mar 10 03:41:26 2023 UTC

Service (Port)	Threat Level
general/tcp	Low
general/icmp	Low

2.6.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

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: 1033892116
Packet 2: 3779769475
```

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

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`

OID:1.3.6.1.4.1.25623.1.0.80091

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

References

`url: http://www.ietf.org/rfc/rfc1323.txt`

`url: http://www.ietf.org/rfc/rfc7323.txt`

`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152`

[return to 192.168.60.254]

2.6.2 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary

The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution:

Solution type: Mitigation

Various mitigations are possible:

. . . continues on next page . . .

. . . continued from previous page . . .

- 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. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method

Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References

```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.60.254]

2.7 192.168.60.4

Host scan start	Fri Mar 10 03:26:15 2023 UTC
Host scan end	Fri Mar 10 03:29:35 2023 UTC

Service (Port)	Threat Level
general/icmp	Low

2.7.1 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary

The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

. . . continued from previous page . . .

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. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References

```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.60.4]