Scan Report

June 28, 2024

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 "metasploitable_CB". The scan started at Fri Jun 28 09:29:08 2024 UTC and ended at . 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
192.168.56.105	4	10	3	0	0
Total: 1	4	10	3	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 17 results selected by the filtering described above. Before filtering there were 198 results.

2 Results per Host

2.1 192.168.56.105

Host scan start Fri Jun 28 09:29:38 2024 UTC
Host scan end

Service (Port)	Threat Level
6697/tcp	High
general/tcp	High
631/tcp	High
80/tcp	Medium
21/tcp	Medium
631/tcp	Medium
22/tcp	Medium
general/icmp	Low
general/tcp	Low
22/tcp	Low

2.1.1 High 6697/tcp

High (CVSS: 8.1)
NVT: UnrealIRCd Authentication Spoofing Vulnerability

Summary
UnrealIRCd is prone to authentication spoofing vulnerability.

Vulnerability Detection Result
`Installed version: 3.2.8.1`
`Fixed version: 3.2.10.7`

Impact
Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.

Solution:
Solution type: VendorFix
Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

Affected Software/OS
UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.

Vulnerability Insight
The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `UnrealIRCd Authentication Spoofing Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.809883
Version used: `2023-07-14T16:09:27Z`

References
`cve: CVE-2016-7144`
`url: http://seclists.org/oss-sec/2016/q3/420`
`url: http://www.securityfocus.com/bid/92763`
`url: http://www.openwall.com/lists/oss-security/2016/09/05/8`
`url: https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b`
`↪c50ba1a34a766`
`url: https://bugs.unrealircd.org/main_page.php`

[return to 192.168.56.105]

2.1.2 High general/tcp

High (CVSS: 10.0)
NVT: Report outdated / end-of-life Scan Engine / Environment (local)

Summary
This script checks and reports an outdated or end-of-life scan engine for the following environments:
- Greenbone Community Edition
- Greenbone Enterprise TRIAL (formerly Greenbone Security Manager TRIAL / Greenbone Community Edition VM)
used for this scan.
NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:
- missing functionalities
- missing bugfixes
- incompatibilities within the feed

Vulnerability Detection Result
```
Version of installed component:          22.4.1 (Installed component: openvas-l
↪ibraries on OpenVAS <= 9, openvas-scanner on Greenbone Community Edition >= 10
↪)
Latest available openvas-scanner version: 23.0.1 (Minimum recommended version, t
↪here are more recent available)
Reference URL(s) for the latest available version: https://forum.greenbone.net/t
↪/greenbone-community-edition-22-4-stable-initial-release-2022-07-25/12638
```

Solution:
Solution type: VendorFix
Update to the latest available stable release for your scan environment.
Note: It is NOT enough to only update the scanner component. All components should be updated to the most recent and stable versions.
Possible solution options depends on the installation method:
- If using the Greenbone Enterprise TRIAL: Please do a new installation with the newest available version
- If using the official Greenbone Community Containers: Please see the references on how to do an update of these
- If the Greenbone Community Edition was build from sources by following the official source build documentation: Please see the references on how to do an update of all components
- If using packages provided by your Linux distribution: Please contact the maintainer of the used distribution / repository and request updated packages
- If using any other installation method: Please contact the provider of this solution
Please check the references for more information.
If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked GSM manual.

Vulnerability Detection Method

. . . continues on next page . . .

... continued from previous page ...

Details: Report outdated / end-of-life Scan Engine / Environment (local)
OID:1.3.6.1.4.1.25623.1.0.108560
Version used: 2024-06-20T05:05:33Z

References

url: https://www.greenbone.net/en/testnow/
url: https://greenbone.github.io/docs/latest/22.4/container/workflows.html#updating-the-greenbone-community-containers
url: https://greenbone.github.io/docs/latest/22.4/source-build/workflows.html#updating-to-newer-releases
url: https://forum.greenbone.net/t/greenbone-community-edition-22-4-stable-initial-release-2022-07-25/12638
url: https://forum.greenbone.net/t/greenbone-community-edition-21-04-end-of-life/13837
url: https://forum.greenbone.net/t/gvm-21-04-end-of-life-initial-release-2021-04-16/8942
url: https://forum.greenbone.net/t/gvm-20-08-end-of-life-initial-release-2020-08-12/6312
url: https://forum.greenbone.net/t/gvm-11-end-of-life-initial-release-2019-10-14/3674
url: https://forum.greenbone.net/t/gvm-10-end-of-life-initial-release-2019-04-05/208
url: https://forum.greenbone.net/t/gvm-9-end-of-life-initial-release-2017-03-07/211
url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/reports.html#creating-an-override

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

Summary

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Vulnerability Detection Result

The "Ubuntu" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:canonical:ubuntu_linux:14.04
Installed version,
build or SP: 14.04
EOL date: 2024-04-01
EOL info: https://wiki.ubuntu.com/Releases

Impact

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: Mitigation
Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method
Checks if an EOL version of an OS is present on the target host.
Details: `Operating System (OS) End of Life (EOL) Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `2024-02-28T14:37:42Z`

[return to 192.168.56.105]

2.1.3 High 631/tcp

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

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

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: 2024-06-14T05:05:48Z

References

cve: CVE-2016-2183
cve: CVE-2016-6329
cve: CVE-2020-12872
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
url: https://sweet32.info/
cert-bund: WID-SEC-2024-1277
cert-bund: WID-SEC-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
cert-bund: WID-SEC-2022-1955
cert-bund: CB-K21/1094
cert-bund: CB-K20/1023
cert-bund: CB-K20/0321
cert-bund: CB-K20/0314
cert-bund: CB-K20/0157
cert-bund: CB-K19/0618
cert-bund: CB-K19/0615
cert-bund: CB-K18/0296
cert-bund: CB-K17/1980
cert-bund: CB-K17/1871
cert-bund: CB-K17/1803
cert-bund: CB-K17/1753
cert-bund: CB-K17/1750
cert-bund: CB-K17/1709
cert-bund: CB-K17/1558
cert-bund: CB-K17/1273
cert-bund: CB-K17/1202
cert-bund: CB-K17/1196
cert-bund: CB-K17/1055
cert-bund: CB-K17/1026
cert-bund: CB-K17/0939
cert-bund: CB-K17/0917
cert-bund: CB-K17/0915
cert-bund: CB-K17/0877
cert-bund: CB-K17/0796
cert-bund: CB-K17/0724
cert-bund: CB-K17/0661
cert-bund: CB-K17/0657
cert-bund: CB-K17/0582
cert-bund: CB-K17/0581
cert-bund: CB-K17/0506

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K17/0504
cert-bund: CB-K17/0467
cert-bund: CB-K17/0345
cert-bund: CB-K17/0098
cert-bund: CB-K17/0089
cert-bund: CB-K17/0086
cert-bund: CB-K17/0082
cert-bund: CB-K16/1837
cert-bund: CB-K16/1830
cert-bund: CB-K16/1635
cert-bund: CB-K16/1630
cert-bund: CB-K16/1624
cert-bund: CB-K16/1622
cert-bund: CB-K16/1500
cert-bund: CB-K16/1465
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2020-2141
dfn-cert: DFN-CERT-2020-0368
dfn-cert: DFN-CERT-2019-1455
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1296
dfn-cert: DFN-CERT-2018-0323
dfn-cert: DFN-CERT-2017-2070
dfn-cert: DFN-CERT-2017-1954
dfn-cert: DFN-CERT-2017-1885
dfn-cert: DFN-CERT-2017-1831
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2017-1785
dfn-cert: DFN-CERT-2017-1626
dfn-cert: DFN-CERT-2017-1326
dfn-cert: DFN-CERT-2017-1239
dfn-cert: DFN-CERT-2017-1238
dfn-cert: DFN-CERT-2017-1090
dfn-cert: DFN-CERT-2017-1060
dfn-cert: DFN-CERT-2017-0968
dfn-cert: DFN-CERT-2017-0947
dfn-cert: DFN-CERT-2017-0946
dfn-cert: DFN-CERT-2017-0904
dfn-cert: DFN-CERT-2017-0816
dfn-cert: DFN-CERT-2017-0746
dfn-cert: DFN-CERT-2017-0677
dfn-cert: DFN-CERT-2017-0675
dfn-cert: DFN-CERT-2017-0611
dfn-cert: DFN-CERT-2017-0609
dfn-cert: DFN-CERT-2017-0522
dfn-cert: DFN-CERT-2017-0519

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2017-0482
dfn-cert: DFN-CERT-2017-0351
dfn-cert: DFN-CERT-2017-0090
dfn-cert: DFN-CERT-2017-0089
dfn-cert: DFN-CERT-2017-0088
dfn-cert: DFN-CERT-2017-0086
```

[return to 192.168.56.105]

2.1.4 Medium 80/tcp

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.6.2
Fixed version:     1.9.0
Installation
path / port:       /phpmyadmin/js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.56.105/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://192.168.56.105/phpmyadmin/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636

... continues on next page ...

... continued from previous page ...

Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590

Medium (CVSS: 6.1)
NVT: jQuery < 1.9.0 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 1.6.2
Fixed version: 1.9.0
Installation
path / port: /phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.56.105/phpmyadmin/setup/../js/jquery/jquery-1.
↪6.2.js
- Referenced at: http://192.168.56.105/phpmyadmin/setup/

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.9.0 XSS Vulnerability

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.141636
Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2012-6708
url: https://bugs.jquery.com/ticket/11290
cert-bund: WID-SEC-2022-0673
cert-bund: CB-K22/0045
cert-bund: CB-K18/1131
dfn-cert: DFN-CERT-2023-1197
dfn-cert: DFN-CERT-2020-0590

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 were identified (URL:input name):
http://192.168.56.105/drupal/:pass
http://192.168.56.105/drupal/?D=A:pass
http://192.168.56.105/payroll_app.php:password
http://192.168.56.105/phpmyadmin/:pma_password
http://192.168.56.105/phpmyadmin/?D=A:pma_password
http://192.168.56.105/phpmyadmin/changelog.php:pma_password
http://192.168.56.105/phpmyadmin/index.php:pma_password
http://192.168.56.105/phpmyadmin/license.php:pma_password
http://192.168.56.105/phpmyadmin/url.php:pma_password

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.

... continues on next page ...

... continued from previous page ...

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

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

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.6.2
Fixed version:     1.6.3
Installation
path / port:       /phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.56.105/phpmyadmin/setup/../js/jquery/jquery-1.
↪6.2.js
- Referenced at:   http://192.168.56.105/phpmyadmin/setup/
```

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.6.3 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2011-4969
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199

Medium (CVSS: 4.3)
NVT: jQuery < 1.6.3 XSS Vulnerability

Summary
jQuery is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 1.6.2
Fixed version: 1.6.3
Installation
path / port: /phpmyadmin/js/jquery/jquery-1.6.2.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.56.105/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at: http://192.168.56.105/phpmyadmin/

Solution:
Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: jQuery < 1.6.3 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: 2023-07-14T05:06:08Z

References
cve: CVE-2011-4969

... continues on next page ...

... continued from previous page ...

```
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
```

[return to 192.168.56.105]

2.1.5 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

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 Password required for openvasvt
Anonymous sessions:     331 Anonymous login ok, send your complete email address
↪ as your password
```

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 without 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: `2023-12-20T05:05:58Z`

[return to 192.168.56.105]

2.1.6 Medium 631/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.
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: `2024-06-14T05:05:48Z`

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
```

. . . continues on next page . . .

... continued from previous page ...

```
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: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-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-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
```

[return to 192.168.56.105]

2.1.7 Medium 22/tcp

Medium (CVSS: 5.3)
NVT: Weak Host Key Algorithm(s) (SSH)

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: `2024-06-14T05:05:48Z`

References
```
url: https://www.rfc-editor.org/rfc/rfc8332
url: https://www.rfc-editor.org/rfc/rfc8709
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.6
```

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

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
```

. . . continues on next page . . .

... continued from previous page ...

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 Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
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 group / 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: `2024-06-14T05:05:48Z`

References
`url: https://weakdh.org/sysadmin.html`
`url: https://www.rfc-editor.org/rfc/rfc9142`
`url: https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem`
`url: https://www.rfc-editor.org/rfc/rfc6194`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.5`

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

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
```

... continues on next page ...

... continued from previous page ...

```
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 [SCHNEIER]. 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 this 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 an 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: `2024-06-14T05:05:48Z`

References

... continues on next page ...

... continued from previous page ...

url: https://www.rfc-editor.org/rfc/rfc8758
url: https://www.kb.cert.org/vuls/id/958563
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3

[return to 192.168.56.105]

2.1.8 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
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

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

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2023-05-11T09:09:33Z

References
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792

... continues on next page ...

... continued from previous page ...

```
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
```

[return to 192.168.56.105]

2.1.9 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure

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

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: 1629113
Packet 2: 1629380
```

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

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091

... continues on next page ...

... continued from previous page ...

Version used: 2023-12-15T16:10:08Z

References

url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 192.168.56.105]

2.1.10 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

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-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

Solution:

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

... continues on next page ...

... continued from previous page ...

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
- 64-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: `2024-06-14T05:05:48Z`

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 192.168.56.105]