Scan Report

April 9, 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 “Ubuntu Scan Metasploitable”. The scan started at Tue Apr 9 04:38:28 2024 UTC and ended at Tue Apr 9 05:12:58 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.2.4	7	12	3	0	0
Total: 1	7	12	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 22 results selected by the filtering described above. Before filtering there were 390 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.2.4	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 10.0.2.4

Host scan start	Tue Apr 9 04:40:52 2024 UTC
Host scan end	Tue Apr 9 05:12:50 2024 UTC

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

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
general/icmp	Low

2.1.1 High 21/tcp

High (CVSS: 10.0)

NVT: ProFTPD ‘mod_copy‘ Unauthenticated Copying Of Files Via SITE CPFR/CPTO

Product detection result

```
cpe:/a:proftpd:proftpd:1.3.5
Detected by ProFTPD Server Version Detection (Remote) (OID: 1.3.6.1.4.1.25623.1.
↪0.900815)
```

Summary

ProFTPD is prone to an unauthenticated copying of files vulnerability.

Quality of Detection: 99

Vulnerability Detection Result

```
The target was found to be vulnerable
```

Impact

Under some circumstances this could result in remote code execution

Solution:

Solution type: VendorFix

Ask the vendor for an update

Vulnerability Detection Method

Try to copy /etc/passwd to /tmp/passwd.copy with SITE CPFR/CPTO
Details: `ProFTPD ‘mod_copy‘ Unauthenticated Copying Of Files Via SITE CPFR/CPTO`
OID:1.3.6.1.4.1.25623.1.0.105254
Version used: `2022-12-02T10:11:16Z`

Product Detection Result

Product: `cpe:/a:proftpd:proftpd:1.3.5`
Method: `ProFTPD Server Version Detection (Remote)`
OID: 1.3.6.1.4.1.25623.1.0.900815)

References

```
cve: CVE-2015-3306
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: http://bugs.proftpd.org/show_bug.cgi?id=4169
cert-bund: CB-K15/0791
cert-bund: CB-K15/0553
dfn-cert: DFN-CERT-2015-0839
dfn-cert: DFN-CERT-2015-0576
```

High (CVSS: 7.5)

NVT: FTP Brute Force Logins Reporting

Summary
It was possible to login into the remote FTP server using weak/known credentials.

Quality of Detection: 95

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
vagrant:vagrant
```

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices

Note: As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: `FTP Brute Force Logins Reporting`
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: `2023-12-06T05:06:11Z`

References

```
cve: CVE-1999-0501
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2001-1594
cve: CVE-2013-7404
cve: CVE-2017-8218
cve: CVE-2018-19063
cve: CVE-2018-19064
```

[return to 10.0.2.4]

2.1.2 High 80/tcp

High (CVSS: 10.0)

NVT: Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check

Summary
Drupal is prone to a remote code execution (RCE) vulnerability.

Quality of Detection: 95

Vulnerability Detection Result

```
Vulnerable URL: http://10.0.2.4/drupal/sites/all/modules/coder/coder_upgrade/scr
↪ipts/coder_upgrade.run.php
```

Solution:
Solution type: VendorFix
Install the latest version.

Vulnerability Insight
The Coder module checks your Drupal code against coding standards and other best practices. It can also fix coding standard violations and perform basic upgrades on modules. The module doesn't sufficiently validate user inputs in a script file that has the php extension. A malicious unauthenticated user can make requests directly to this file to execute arbitrary php code.

Vulnerability Detection Method
Checks for known error message from affected modules.
Details: `Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.105818
Version used: `2023-07-21T05:05:22Z`

References
url: https://www.drupal.org/node/2765575

High (CVSS: 7.5)

NVT: Test HTTP dangerous methods

Summary
Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.

Quality of Detection: 99

Vulnerability Detection Result

```
We could upload the following files via the PUT method at this web server:
http://10.0.2.4/uploads/puttest172099026.html
We could delete the following files via the DELETE method at this web server:
http://10.0.2.4/uploads/puttest172099026.html
```

Impact
- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution:
Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Affected Software/OS
Web servers with enabled PUT and/or DELETE methods.

Vulnerability Detection Method
Checks if dangerous HTTP methods such as PUT and DELETE are enabled and can be misused to upload or delete files.
Details: `Test HTTP dangerous methods`
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: `2023-08-01T13:29:10Z`

References

```
url: http://www.securityfocus.com/bid/12141
owasp: OWASP-CM-001
```

High (CVSS: 7.5)

NVT: Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

Drupal is prone to an SQL injection (SQLi) vulnerability.

Quality of Detection: 98

Vulnerability Detection Result

```
Vulnerable URL: http://10.0.2.4/drupal/?q=node&destination=node
```

Impact

Exploiting this issue could allow an attacker to execute arbitrary code, to gain elevated privileges and to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Solution:

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

Drupal 7.x versions prior to 7.32 are vulnerable.

Vulnerability Insight

Drupal fails to sufficiently sanitize user-supplied data before using it in an SQL query.

Vulnerability Detection Method

Sends a special crafted HTTP POST request and checks the response.

Details: `Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check`

OID:1.3.6.1.4.1.25623.1.0.105101

Version used: `2023-07-26T05:05:09Z`

References

```
cve: CVE-2014-3704
url: https://www.drupal.org/forum/newsletters/security-advisories-for-drupal-cor
↪e/2014-10-15/sa-core-2014-005-drupal-core-sql
url: http://www.securityfocus.com/bid/70595
cert-bund: CB-K14/1301
cert-bund: CB-K14/0920
dfn-cert: DFN-CERT-2014-1369
dfn-cert: DFN-CERT-2014-0958
```

[return to 10.0.2.4]

2.1.3 High 22/tcp

High (CVSS: 9.8)

NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.

Quality of Detection: 95

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
vagrant:vagrant
```

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight
As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `2024-03-15T05:06:15Z`

References

```
cve: CVE-1999-0501
cve: CVE-1999-0502
cve: CVE-1999-0507
cve: CVE-1999-0508
cve: CVE-2020-9473
cve: CVE-2023-1944
cve: CVE-2024-22902
```

[return to 10.0.2.4]

2.1.4 High general/tcp

High (CVSS: 10.0)

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

Product detection result

```
cpe:/o:canonical:ubuntu_linux:14.04
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

Summary

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

Quality of Detection: 80

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.

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`

Product Detection Result

Product: `cpe:/o:canonical:ubuntu_linux:14.04`

Method: `OS Detection Consolidation and Reporting`

OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 10.0.2.4]

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.

Quality of Detection: 70

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 10.0.2.4]

2.1.6 Medium 80/tcp

Medium (CVSS: 6.1)

NVT: jQuery < 1.9.0 XSS Vulnerability

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection: 80

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://10.0.2.4/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://10.0.2.4/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
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.

Quality of Detection: 80

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://10.0.2.4/phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
- Referenced at:   http://10.0.2.4/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`
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0590
```

Medium (CVSS: 5.0)

NVT: Unprotected Web App / Device Installers (HTTP)

Summary
The script attempts to identify installation/setup pages of various web apps/devices that are publicly accessible and not protected by e.g. account restrictions or having their setup finished.

Quality of Detection: 80

Vulnerability Detection Result

```
The following web app/device installers are unprotected/have not finished their
↪setup and are publicly accessible (URL:Description):
http://10.0.2.4/phpmyadmin/setup/index.php - CubeCart / phpMyAdmin installer
```

Impact
It is possible to install or reconfigure the software. In doing so, the attacker could overwrite existing configurations. It could be possible for the attacker to gain access to the base system

Solution:
Solution type: Mitigation
Setup and/or installation pages for Web Apps should not be publicly accessible via a web server. Restrict access to it, remove it completely or finish the setup of the application / device.

Vulnerability Detection Method
Enumerate the remote web server and check if unprotected web apps/devices are accessible for installation.
Details: `Unprotected Web App / Device Installers (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.107307
Version used: `2024-03-07T05:06:18Z`

Medium (CVSS: 5.0)

NVT: Drupal 7.0 Information Disclosure Vulnerability - Active Check

Summary
Drupal is prone to an information disclosure vulnerability.

Quality of Detection: 95

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

```
Vulnerable URL: http://10.0.2.4/drupal/modules/simpletest/tests/upgrade/drupal-6
↪.upload.database.php
```

Impact

Successful exploitation will allow attacker to obtain sensitive information that could aid in further attacks.

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

Drupal version 7.0 is known to be affected.

Vulnerability Insight

The flaw is due to insufficient error checking, allows remote attackers to obtain sensitive information via a direct request to a .php file, which reveals the installation path in an error message.

Vulnerability Detection Method

Details: `Drupal 7.0 Information Disclosure Vulnerability - Active Check`

OID:1.3.6.1.4.1.25623.1.0.902574

Version used: `2021-12-01T11:10:56Z`

References

```
cve: CVE-2011-3730
url: http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/!_README
url: http://code.google.com/p/inspathx/source/browse/trunk/paths_vuln/drupal-7.0
```

Medium (CVSS: 5.0)

NVT: Sensitive File Disclosure (HTTP)

Summary

The script attempts to identify files containing sensitive data at the remote web server.

Quality of Detection: 70

Vulnerability Detection Result

```
The following files containing sensitive information were identified:
Description:   Microsoft IIS / ASP.NET Core Module web.config file accessible. T
↪his could contain sensitive information about the structure of the application
↪ / web server and shouldn't be accessible.
Match:         <configuration>
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
  <system.webServer>
Used regex:     ^\s*<(configuration|system\.web(Server)?)>
Extra match 1:    </system.webServer>
</configuration>
Used regex:     ^\s*</(configuration|system\.web(Server)?)>
URL:            http://10.0.2.4/drupal/web.config
```

Impact

Based on the information provided in these files an attacker might be able to gather additional info and/or sensitive data like usernames and passwords.

Solution:

Solution type: Mitigation

The sensitive files shouldn't be accessible via a web server. Restrict access to it or remove it completely.

Vulnerability Insight

Currently the script is checking for files like e.g.:
- Software (Blog, CMS) configuration or log files
- Web / application server configuration / password files (.htaccess, .htpasswd, web.config, web.xml, ...)
- Cloud (e.g. AWS) configuration files
- Files containing API keys for services / providers
- Database backup files
- Editor / history files
- SSH or SSL/TLS Private Keys

Vulnerability Detection Method

Enumerate the remote web server and check if sensitive files are accessible.

Details: `Sensitive File Disclosure (HTTP)`

OID:1.3.6.1.4.1.25623.1.0.107305

Version used: `2023-11-09T05:05:33Z`

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

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

Quality of Detection: 80

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://10.0.2.4/drupal/:pass
http://10.0.2.4/drupal/?D=A:pass
http://10.0.2.4/payroll_app.php:password
http://10.0.2.4/phpmyadmin/:pma_password
http://10.0.2.4/phpmyadmin/?D=A:pma_password
http://10.0.2.4/phpmyadmin/changelog.php:pma_password
http://10.0.2.4/phpmyadmin/index.php:pma_password
http://10.0.2.4/phpmyadmin/license.php:pma_password
http://10.0.2.4/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.

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.

Quality of Detection: 80

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://10.0.2.4/phpmyadmin/setup/../js/jquery/jquery-1.6.2.js
- Referenced at:   http://10.0.2.4/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
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
dfn-cert: DFN-CERT-2016-0890
```

Medium (CVSS: 4.3)

NVT: jQuery < 1.6.3 XSS Vulnerability

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

Quality of Detection: 80

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://10.0.2.4/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://10.0.2.4/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
url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/
cert-bund: CB-K17/0195
dfn-cert: DFN-CERT-2017-0199
dfn-cert: DFN-CERT-2016-0890
```

[return to 10.0.2.4]

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).

Quality of Detection: 80

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: `2023-10-12T05:05:32Z`

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).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
```

. . . continues on next page . . .

... continued from previous page ...

```
KEX algorithm                      | Reason
--------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact

An attacker can quickly break individual connections.

Solution:

Solution type: Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Vulnerability Insight

- 1024-bit MODP group / prime KEX algorithms:

Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for 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: `2023-10-12T05:05:32Z`

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).

Quality of Detection: 80

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Vulnerability Insight
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [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.

. . . continues on next page . . .

. . . continued from previous page . . .

- 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: `2023-10-12T05:05:32Z`

References

```
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 10.0.2.4]

2.1.8 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).

Quality of Detection: 80

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):
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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).

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: `2023-10-12T05:05:32Z`

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

[return to 10.0.2.4]

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.

Quality of Detection: 80

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 7396597
Packet 2: 7396862
```

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

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

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

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

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

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

[return to 10.0.2.4]

2.1.10 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result

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

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

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

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

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

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 10.0.2.4]

This file was automatically generated.