Scan Report

March 22, 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 “Immediate scan of IP 192.168.116.131”. The scan started at Fri Mar 22 06:53:08 2024 UTC and ended at Fri Mar 22 07:22:55 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
192.168.116.131	7	13	3	0	0
Total: 1	7	13	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 23 results selected by the filtering described above. Before filtering there were 414 results.

1.1 Host Authentications

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

2 Results per Host

2.1 192.168.116.131

Host scan start	Fri Mar 22 06:53:49 2024 UTC
Host scan end	Fri Mar 22 07:22:46 2024 UTC

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

. . . (continues) . . .

. . . (continued) . . .

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

2.1.1 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://192.168.116.131/drupal/sites/all/modules/coder/coder_upgr
↪ade/scripts/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: Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check

. . . continues on next page . . .

. . . continued from previous page . . .

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

Quality of Detection: 98

Vulnerability Detection Result

```
Vulnerable URL: http://192.168.116.131/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
```

High (CVSS: 7.5)

NVT: Test HTTP dangerous methods

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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://192.168.116.131/uploads/puttest726997747.html
We could delete the following files via the DELETE method at this web server:
http://192.168.116.131/uploads/puttest726997747.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
```

[return to 192.168.116.131]

2.1.2 High 6697/tcp

High (CVSS: 8.1)

NVT: UnrealIRCd Authentication Spoofing Vulnerability

Product detection result

. . . continues on next page . . .

. . . continued from previous page . . .

```
cpe:/a:unrealircd:unrealircd:3.2.8.1
Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
```

Summary
UnrealIRCd is prone to authentication spoofing vulnerability.

Quality of Detection: 80

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`

Product Detection Result
Product: `cpe:/a:unrealircd:unrealircd:3.2.8.1`
Method: `UnrealIRCd Detection`
OID: 1.3.6.1.4.1.25623.1.0.809884)

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

url: https://bugs.unrealircd.org/main_page.php

High (CVSS: 7.5)

NVT: UnrealIRCd Backdoor

Summary
Detection of backdoor in UnrealIRCd.

Quality of Detection: 70

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

Solution:
Solution type: VendorFix
Install latest version of unrealircd and check signatures of software you're installing.

Affected Software/OS
The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

Vulnerability Insight
Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.

Vulnerability Detection Method
Details: UnrealIRCd Backdoor
OID:1.3.6.1.4.1.25623.1.0.80111
Version used: 2023-08-01T13:29:10Z

References
cve: CVE-2010-2075
url: http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt
url: http://seclists.org/fulldisclosure/2010/Jun/277
url: http://www.securityfocus.com/bid/40820

[return to 192.168.116.131]

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.

Quality of Detection: 98

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
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `2023-07-20T05:05:17Z`

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-2024-0209
cert-bund: WID-SEC-2024-0064
cert-bund: WID-SEC-2022-2226
```

... continues on next page ...

. . . continued from previous page . . .

```
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
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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K16/1307
cert-bund: CB-K16/1296
dfn-cert: DFN-CERT-2021-1618
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2021-0770
dfn-cert: DFN-CERT-2021-0274
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
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
dfn-cert: DFN-CERT-2016-1943
dfn-cert: DFN-CERT-2016-1937
dfn-cert: DFN-CERT-2016-1732
dfn-cert: DFN-CERT-2016-1726
dfn-cert: DFN-CERT-2016-1715
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2016-1714
dfn-cert: DFN-CERT-2016-1588
dfn-cert: DFN-CERT-2016-1555
dfn-cert: DFN-CERT-2016-1391
dfn-cert: DFN-CERT-2016-1378
```

[return to 192.168.116.131]

2.1.4 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)`

. . . continues on next page . . .

. . . continued from previous page . . .

OID: 1.3.6.1.4.1.25623.1.0.900815)

References

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

[return to 192.168.116.131]

2.1.5 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`

. . . continues on next page . . .

. . . continued from previous page . . .

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):
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

. . . continues on next page . . .

. . . continued from previous page . . .

- 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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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: `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 192.168.116.131]

2.1.6 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.

Quality of Detection: 80

. . . continues on next page . . .

. . . continued from previous page . . .

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://192.168.116.131/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://192.168.116.131/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

. . . 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/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://192.168.116.131/phpmyadmin/setup/../js/jquery/jquery-1
↪.6.2.js
- Referenced at:   http://192.168.116.131/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
dfn-cert: DFN-CERT-2020-0590
```

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>
  <system.webServer>
Used regex:    ^\s*<(configuration|system\.web(Server)?)>
Extra match 1:   </system.webServer>
</configuration>
Used regex:    ^\s*</(configuration|system\.web(Server)?)>
URL:           http://192.168.116.131/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

. . . continues on next page . . .

. . . continued from previous page . . .

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

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

```
Vulnerable URL: http://192.168.116.131/drupal/modules/simpletest/tests/upgrade/d
↪rupal-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: 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://192.168.116.131/phpmyadmin/setup/index.php - CubeCart / phpMyAdmin instal
↪ler
```

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: 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):
http://192.168.116.131/drupal/:pass
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://192.168.116.131/drupal/?D=A:pass
http://192.168.116.131/payroll_app.php:password
http://192.168.116.131/phpmyadmin/:pma_password
http://192.168.116.131/phpmyadmin/?D=A:pma_password
http://192.168.116.131/phpmyadmin/changelog.php:pma_password
http://192.168.116.131/phpmyadmin/index.php:pma_password
http://192.168.116.131/phpmyadmin/license.php:pma_password
http://192.168.116.131/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

. . . 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:     1.6.3
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://192.168.116.131/phpmyadmin/setup/../js/jquery/jquery-1
↪.6.2.js
- Referenced at:   http://192.168.116.131/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.

. . . continues on next page . . .

. . . continued from previous page . . .

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://192.168.116.131/phpmyadmin/js/jquery/jquery-1.6.2.js
- Referenced at:   http://192.168.116.131/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 192.168.116.131]

2.1.7 Medium 631/tcp

Medium (CVSS: 4.3)

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Quality of Detection: 98

Vulnerability Detection Result

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

Impact

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

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

Solution:

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more 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: `2023-10-20T16:09:12Z`

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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-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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 192.168.116.131]

2.1.8 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

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `2023-12-20T05:05:58Z`

[return to 192.168.116.131]

2.1.9 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):
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.

. . . continues on next page . . .

. . . continued from previous page . . .

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 192.168.116.131]

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

. . . continues on next page . . .

. . . continued from previous page . . .

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 192.168.116.131]

2.1.11 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.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 122663
Packet 2: 122938
```

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.

. . . continues on next page . . .

... continued from previous page ...

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/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 192.168.116.131]