Scan Report

January 27, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 172.16.1.7". The scan started at Mon Jan 16 15:18:07 2023 UTC and ended at Mon Jan 16 15:44:59 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
172.16.1.7	17	43	2	0	0
Total: 1	17	43	2	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 62 results selected by the filtering described above. Before filtering there were 313 results.

2 Results per Host

2.1 172.16.1.7

Host scan start	Mon Jan 16 15:18:59 2023 UTC
Host scan end	Mon Jan 16 15:44:53 2023 UTC

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

2.1.1 High 443/tcp

High (CVSS: 9.8)
NVT: WordPress Photo Gallery Plugin < 1.6.0 SQLi Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to an SQL injection (SQLi) vulnerability.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
Installed version: 1.5.34
Fixed version: 1.6.0
Installation
path / port: /wp-content/plugins/photo-gallery

Solution:
Solution type: VendorFix
Update to version 1.6.0 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.6.0.

Vulnerability Insight
The plugin does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Photo Gallery Plugin < 1.6.0 SQLi Vulnerability
OID:1.3.6.1.4.1.25623.1.0.147923
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2022-0169
url: https://wpscan.com/vulnerability/0b4d870f-eab8-4544-91f8-9c5f0538709c

High (CVSS: 9.8)
NVT: WordPress Photo Gallery Plugin < 1.5.55 SQLi Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to an SQL injection (SQLi) vulnerability.

Vulnerability Detection Result
Installed version: 1.5.34
Fixed version: 1.5.55
Installation
path / port: /wp-content/plugins/photo-gallery

Solution:
Solution type: VendorFix
Update to version 1.5.55 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.55.

Vulnerability Insight
Unvalidated input leads to SQL injection via the frontend/models/model.php bwg_search_x parameter.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.55 SQLi Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.145615
Version used: `2022-07-19T10:11:08Z`

References
`cve: CVE-2021-24139`
`url: https://wpscan.com/vulnerability/2e33088e-7b93-44af-aa6a-e5d924f86e28`
`url: https://wordpress.org/plugins/photo-gallery/#developers`

High (CVSS: 9.8)
NVT: WordPress Photo Gallery Plugin < 1.6.3 Multiple Vulnerabilities

Summary
The WordPress plugin 'Photo Gallery' is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.6.3
Installation
path / port:       /wp-content/plugins/photo-gallery
```

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

Affected Software/OS
WordPress Photo Gallery plugin prior to version 1.6.3.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-1281: SQL Injection
- CVE-2022-1282: Cross-site Scripting (XSS)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: WordPress Photo Gallery Plugin < 1.6.3 Multiple Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.124064
Version used: 2022-07-20T10:33:02Z

References
cve: CVE-2022-1281
cve: CVE-2022-1282
url: https://wpscan.com/vulnerability/2b4866f2-f511-41c6-8135-cf1e0263d8de
url: https://wpscan.com/vulnerability/37a58f4e-d2bc-4825-8e1b-4aaf0a1cf1b6

High (CVSS: 9.0)
NVT: WordPress Gwolle Guestbook Plugin < 1.5.4 RFI Vulnerability

Summary
The WordPress plugin 'Gwolle Guestbook' is prone to a remote file inclusion (RFI) vulnerability.

Vulnerability Detection Result
Installed version: 1.5.3
Fixed version: 1.5.4
Installation
path / port: /wp-content/plugins/gwolle-gb

Impact
Successful exploitation of this vulnerability will lead to entire WordPress installation compromise, and may even lead to the entire web server compromise.

Solution:
Solution type: VendorFix
Update to version 1.5.4 or later.

Affected Software/OS
WordPress Gwolle Guestbook plugin before 1.5.4.

Vulnerability Insight
HTTP GET parameter 'abspath' of frontend/captcha/ajaxresponse.php is not being properly sanitized before being used in PHP require() function leading to a PHP remote file inclusion vulnerability.
A remote attacker can include a file named 'wp-load.php' from arbitrary remote server and execute its content on the vulnerable web server.
In order to do so the attacker needs to place a malicious 'wp-load.php' file into his server document root and includes server's URL into request:
http://example.com/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://[hackers_
In order to exploit this vulnerability 'allow_url_include' shall be set to 1. Otherwise, attacker may still include local files and also execute arbitrary code.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Gwolle Guestbook Plugin < 1.5.4 RFI Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112042
Version used: `2022-11-14T10:12:51Z`

References
`cve: CVE-2015-8351`
`url: https://wordpress.org/plugins/gwollegb/#changelog`
`url: https://packetstormsecurity.com/files/134599/WordPress-Gwolle-Guestbook-1.5.3-Remote-File-Inclusion.html`

High (CVSS: 8.8)
NVT: WordPress Contact Form Builder Plugin < 1.0.69 CSRF Vulnerability

Summary
The WordPress plugin 'Contact Form Builder' is prone to a CSRF vulnerability.

Vulnerability Detection Result
`Installed version: 1.0.67`
`Fixed version: 1.0.69`
`Installation path / port: /wp-content/plugins/contact-form-builder`

Solution:
Solution type: VendorFix
Update to version 1.0.69 or later.

Affected Software/OS
WordPress Contact Form Builder plugin before version 1.0.69.

Vulnerability Insight
The plugin allows CSRF via the wp-admin/admin-ajax.php action parameter, resulting in a local file inclusion via directory traversal, because there can be a discrepancy between the $_POST['action'] value and the $_GET['action'] value, with the latter being unsanitized.

Vulnerability Detection Method
Details: `WordPress Contact Form Builder Plugin < 1.0.69 CSRF Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112569
Version used: `2022-07-19T10:11:08Z`

References
`cve: CVE-2019-11557`
`url: https://lists.openwall.net/full-disclosure/2019/04/23/1`
`url: https://wordpress.org/plugins/contact-form-builder/#developers`

High (CVSS: 7.8)
NVT: WordPress Multiple Plugins / Themes Directory Traversal / File Download Vulnerability (HTTP)

Summary
Multiple WordPress Plugins / Themes are prone to a directory traversal or file download vulnerability.

Vulnerability Detection Result
The following URLs are vulnerable:
https://172.16.1.7/wp-content/plugins/site-import/admin/page.php?url=..%2F..%2F.
↪.%2F..%2Fwp-config.php
https://172.16.1.7/wp-content/plugins/site-import/admin/page.php?url=..%2F..%2F.
↪.%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc/passwd
https://172.16.1.7/wp-content/plugins/localize-my-post/ajax/include.php?file=../
↪../../../../../../../../../etc/passwd
https://172.16.1.7/wp-content/plugins/site-editor/editor/extensions/pagebuilder/
↪includes/ajax_shortcode_pattern.php?ajax_path=../../../../../../../../../../et
↪c/passwd

Impact
Successful exploitation will allow a remote attacker to download arbitrary files.

Solution:
Solution type: VendorFix
Please contact the vendor for additional information regarding potential updates. If none exist, remove the plugin / theme.

Affected Software/OS
The following WordPress Plugins / Themes are known to be affected:
- Product Input Fields for WooCommerce
- Slider Revolution (revslider)
- MiwoFTP
- aspose-doc-exporter
- candidate-application-form
- cloudsafe365-for-wp
- db-backup
- google-mp3-audio-player
- hb-audio-gallery-lite
- history-collection
- old-post-spinner
- pica-photo-gallery
- pictpress
- recent-backups
- wptf-image-gallery
- mTheme-Unus
- parallelus-mingle

... continues on next page ...

... continued from previous page ...

- parallelus-salutation
- tinymce-thumbnail-gallery
- simple-image-manipulator
- site-import
- robotcpa
- Duplicator (Free and Pro)
- mypixs
- Membership Simplified (membership-simplified-for-oap-members-only)
- ibs-Mappro
- wp-ecommerce-shop-styling
- wp-swimteam
- mdc-youtube-downloader
- image-export
- zip-attachments
- download-zip-attachments
- se-html5-album-audio-player
- wp-instance-rename
- wp-license.php (unknown plugin)
- adaptive-images
- gracemedia-media-player
- localize-my-post
- site-editor
- wechat-broadcast
- simple-fields
- tutor
- mail-masta
- wp-vault
- wpsite-background-takeover
- NativeChurch
- wordfence
- memphis-documents-library
- advanced-dewplayer
- dukapress
- wp-source-control
- tera-charts
- Zoomsounds
- admin-word-count-column
- ad-widget
- amministrazione-aperta
- aspose-cloud-ebook-generator
- aspose-importer-exporter
- aspose-pdf-exporter
- brandfolder
- cab-fare-calculator
- cherry-plugin
- church-admin
- churchope

... continues on next page ...

... continued from previous page ...

- shortcode
- sniplets
- video-synchro-pdf
- oxygen-theme
- count-per-day
- ebook-download
- simple-file-list
- Javo Spot Premium Theme

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `WordPress Multiple Plugins / Themes Directory Traversal / File Download Vulnera.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.117055
Version used: `2022-08-09T10:11:17Z`

References
`cve: CVE-2007-6369`
`cve: CVE-2012-0896`
`cve: CVE-2013-7240`
`cve: CVE-2014-4940`
`cve: CVE-2014-5368`
`cve: CVE-2014-8799`
`cve: CVE-2014-9119`
`cve: CVE-2014-9734`
`cve: CVE-2015-1000005`
`cve: CVE-2015-1000006`
`cve: CVE-2015-1000007`
`cve: CVE-2015-1000010`
`cve: CVE-2015-1000012`
`cve: CVE-2015-1579`
`cve: CVE-2015-4414`
`cve: CVE-2015-4694`
`cve: CVE-2015-4703`
`cve: CVE-2015-4704`
`cve: CVE-2015-5468`
`cve: CVE-2015-5469`
`cve: CVE-2015-5471`
`cve: CVE-2015-5472`
`cve: CVE-2015-5609`
`cve: CVE-2015-9406`
`cve: CVE-2015-9470`
`cve: CVE-2015-9480`
`cve: CVE-2016-10924`
`cve: CVE-2016-10956`
`cve: CVE-2017-1002008`
`cve: CVE-2018-16283`

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2018-16299
cve: CVE-2018-7422
cve: CVE-2018-9118
cve: CVE-2019-14205
cve: CVE-2019-14206
cve: CVE-2019-9618
cve: CVE-2020-11738
cve: CVE-2021-39316
cve: CVE-2022-1119
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
```

High (CVSS: 7.8)
NVT: WordPress Duplicator Plugin < 1.4.7 Information Disclosure Vulnerability

Summary
The WordPress plugin Duplicator is prone to an information disclosure vulnerability.

Vulnerability Detection Result

```
Installed version: 1.2.32
Fixed version:     1.4.7
Installation
path / port:       /wp-content/plugins/duplicator
```

Solution:
Solution type: VendorFix
Update to version 1.4.7 or later.

Affected Software/OS
WordPress Duplicator plugin version prior to 1.4.7.

Vulnerability Insight
The Duplicator WordPress plugin discloses the url of the a backup to unauthenticated visitors accessing the main installer endpoint of the plugin, if the installer script has been run once by an administrator, allowing download of the full site backup without authenticating.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Duplicator Plugin < 1.4.7 Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.124143
Version used: `2022-08-25T10:12:37Z`

References

```
cve: CVE-2022-2551
url: https://wpscan.com/vulnerability/f27d753e-861a-4d8d-9b9a-6c99a8a7ebe0
url: https://github.com/SecuriTrust/CVEsLab/tree/main/CVE-2022-2551
```

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_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
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: `2022-08-01T10:11:45Z`

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-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

High (CVSS: 7.5)
NVT: WordPress iThemes Security Plugin < 7.7.0 Incorrect Authorization Vulnerability

Summary
The WordPress plugin 'iThemes Security' enforces authorization rules incorrectly.

Vulnerability Detection Result
Installed version: 7.0.2
Fixed version: 7.7.0
Installation
path / port: /wp-content/plugins/better-wp-security

Impact
If the password requirements are not properly enforced, users may use insecure passwords that can easily be cracked by malicious actors.

Solution:
Solution type: VendorFix
Update to version 7.7.0 or later.

Affected Software/OS
WordPress iThemes Security plugin through version 7.6.1.

Vulnerability Insight
The plugin does not enforce new password requirements on already existing accounts until after the second login.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress iThemes Security Plugin < 7.7.0 Incorrect Authorization Vulnerability
OID:1.3.6.1.4.1.25623.1.0.113811
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2020-36176
url: https://wordpress.org/plugins/better-wp-security/#developers

[return to 172.16.1.7]

2.1.2 High 80/tcp

High (CVSS: 9.8)
NVT: WordPress Photo Gallery Plugin < 1.6.0 SQLi Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to an SQL injection (SQLi) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.6.0
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.6.0 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.6.0.

Vulnerability Insight
The plugin does not validate and escape the bwg_tag_id_bwg_thumbnails_0 parameter before using it in a SQL statement via the bwg_frontend_data AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL injection.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.6.0 SQLi Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.147923
Version used: `2022-07-19T10:11:08Z`

References
```
cve: CVE-2022-0169
url: https://wpscan.com/vulnerability/0b4d870f-eab8-4544-91f8-9c5f0538709c
```

High (CVSS: 9.8)
NVT: WordPress Photo Gallery Plugin < 1.5.55 SQLi Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to an SQL injection (SQLi) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.5.55
```

... continues on next page ...

... continued from previous page ...

```
Installation
path / port:        /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.5.55 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.55.

Vulnerability Insight
Unvalidated input leads to SQL injection via the frontend/models/model.php bwg_search_x parameter.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.55 SQLi Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.145615
Version used: `2022-07-19T10:11:08Z`

References
`cve: CVE-2021-24139`
`url: https://wpscan.com/vulnerability/2e33088e-7b93-44af-aa6a-e5d924f86e28`
`url: https://wordpress.org/plugins/photo-gallery/#developers`

High (CVSS: 9.8)
NVT: WordPress Photo Gallery Plugin < 1.6.3 Multiple Vulnerabilities

Summary
The WordPress plugin 'Photo Gallery' is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.34
Fixed version:     1.6.3
Installation
path / port:       /wp-content/plugins/photo-gallery
```

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

Affected Software/OS
WordPress Photo Gallery plugin prior to version 1.6.3.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2022-1281: SQL Injection
- CVE-2022-1282: Cross-site Scripting (XSS)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.6.3 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.124064
Version used: `2022-07-20T10:33:02Z`

References
`cve: CVE-2022-1281`
`cve: CVE-2022-1282`
`url: https://wpscan.com/vulnerability/2b4866f2-f511-41c6-8135-cf1e0263d8de`
`url: https://wpscan.com/vulnerability/37a58f4e-d2bc-4825-8e1b-4aaf0a1cf1b6`

High (CVSS: 9.0)
NVT: WordPress Gwolle Guestbook Plugin < 1.5.4 RFI Vulnerability

Summary
The WordPress plugin 'Gwolle Guestbook' is prone to a remote file inclusion (RFI) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.3
Fixed version:     1.5.4
Installation
path / port:       /wp-content/plugins/gwolle-gb
```

Impact
Successful exploitation of this vulnerability will lead to entire WordPress installation compromise, and may even lead to the entire web server compromise.

Solution:
Solution type: VendorFix
Update to version 1.5.4 or later.

Affected Software/OS
WordPress Gwolle Guestbook plugin before 1.5.4.

Vulnerability Insight
HTTP GET parameter 'abspath' of frontend/captcha/ajaxresponse.php is not being properly sanitized before being used in PHP require() function leading to a PHP remote file inclusion vulnerability.
A remote attacker can include a file named 'wp-load.php' from arbitrary remote server and execute its content on the vulnerable web server.

... continues on next page ...

... continued from previous page ...

In order to do so the attacker needs to place a malicious 'wp-load.php' file into his server document root and includes server's URL into request:
http://example.com/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://[hackers_
In order to exploit this vulnerability 'allow_url_include' shall be set to 1. Otherwise, attacker may still include local files and also execute arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Gwolle Guestbook Plugin < 1.5.4 RFI Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112042
Version used: `2022-11-14T10:12:51Z`

References
`cve: CVE-2015-8351`
`url: https://wordpress.org/plugins/gwollegb/#changelog`
`url: https://packetstormsecurity.com/files/134599/WordPress-Gwolle-Guestbook-1.5`
`↪.3-Remote-File-Inclusion.html`

High (CVSS: 8.8)
NVT: WordPress Contact Form Builder Plugin < 1.0.69 CSRF Vulnerability

Summary
The WordPress plugin 'Contact Form Builder' is prone to a CSRF vulnerability.

Vulnerability Detection Result
`Installed version: 1.0.67`
`Fixed version: 1.0.69`
`Installation`
`path / port: /wp-content/plugins/contact-form-builder`

Solution:
Solution type: VendorFix
Update to version 1.0.69 or later.

Affected Software/OS
WordPress Contact Form Builder plugin before version 1.0.69.

Vulnerability Insight
The plugin allows CSRF via the wp-admin/admin-ajax.php action parameter, resulting in a local file inclusion via directory traversal, because there can be a discrepancy between the $_POST['action'] value and the $_GET['action'] value, with the latter being unsanitized.

Vulnerability Detection Method
Details: `WordPress Contact Form Builder Plugin < 1.0.69 CSRF Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112569

... continues on next page ...

... continued from previous page ...

Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2019-11557
url: https://lists.openwall.net/full-disclosure/2019/04/23/1
url: https://wordpress.org/plugins/contact-form-builder/#developers

High (CVSS: 7.8)
NVT: WordPress Multiple Plugins / Themes Directory Traversal / File Download Vulnerability (HTTP)

Summary
Multiple WordPress Plugins / Themes are prone to a directory traversal or file download vulnerability.

Vulnerability Detection Result
The following URLs are vulnerable:
http://172.16.1.7/wp-content/plugins/site-import/admin/page.php?url=..%2F..%2F..
↪%2F..%2Fwp-config.php
http://172.16.1.7/wp-content/plugins/site-import/admin/page.php?url=..%2F..%2F..
↪%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc/passwd
http://172.16.1.7/wp-content/plugins/localize-my-post/ajax/include.php?file=../.
↪./../../../../../../../../etc/passwd
http://172.16.1.7/wp-content/plugins/site-editor/editor/extensions/pagebuilder/i
↪ncludes/ajax_shortcode_pattern.php?ajax_path=../../../../../../../../../../etc
↪/passwd

Impact
Successful exploitation will allow a remote attacker to download arbitrary files.

Solution:
Solution type: VendorFix
Please contact the vendor for additional information regarding potential updates. If none exist, remove the plugin / theme.

Affected Software/OS
The following WordPress Plugins / Themes are known to be affected:
- Product Input Fields for WooCommerce
- Slider Revolution (revslider)
- MiwoFTP
- aspose-doc-exporter
- candidate-application-form
- cloudsafe365-for-wp
- db-backup
- google-mp3-audio-player
- hb-audio-gallery-lite

... continues on next page ...

... continued from previous page ...

- history-collection
- old-post-spinner
- pica-photo-gallery
- pictpress
- recent-backups
- wptf-image-gallery
- mTheme-Unus
- parallelus-mingle
- parallelus-salutation
- tinymce-thumbnail-gallery
- simple-image-manipulator
- site-import
- robotcpa
- Duplicator (Free and Pro)
- mypixs
- Membership Simplified (membership-simplified-for-oap-members-only)
- ibs-Mappro
- wp-ecommerce-shop-styling
- wp-swimteam
- mdc-youtube-downloader
- image-export
- zip-attachments
- download-zip-attachments
- se-html5-album-audio-player
- wp-instance-rename
- wp-license.php (unknown plugin)
- adaptive-images
- gracemedia-media-player
- localize-my-post
- site-editor
- wechat-broadcast
- simple-fields
- tutor
- mail-masta
- wp-vault
- wpsite-background-takeover
- NativeChurch
- wordfence
- memphis-documents-library
- advanced-dewplayer
- dukapress
- wp-source-control
- tera-charts
- Zoomsounds
- admin-word-count-column
- ad-widget
- amministrazione-aperta

... continues on next page ...

... continued from previous page ...

- aspose-cloud-ebook-generator
- aspose-importer-exporter
- aspose-pdf-exporter
- brandfolder
- cab-fare-calculator
- cherry-plugin
- church-admin
- churchope
- shortcode
- sniplets
- video-synchro-pdf
- oxygen-theme
- count-per-day
- ebook-download
- simple-file-list
- Javo Spot Premium Theme

Vulnerability Detection Method

Sends a crafted HTTP GET request and checks the response.

Details: `WordPress Multiple Plugins / Themes Directory Traversal / File Download Vulnera.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.117055

Version used: `2022-08-09T10:11:17Z`

References

`cve: CVE-2007-6369`
`cve: CVE-2012-0896`
`cve: CVE-2013-7240`
`cve: CVE-2014-4940`
`cve: CVE-2014-5368`
`cve: CVE-2014-8799`
`cve: CVE-2014-9119`
`cve: CVE-2014-9734`
`cve: CVE-2015-1000005`
`cve: CVE-2015-1000006`
`cve: CVE-2015-1000007`
`cve: CVE-2015-1000010`
`cve: CVE-2015-1000012`
`cve: CVE-2015-1579`
`cve: CVE-2015-4414`
`cve: CVE-2015-4694`
`cve: CVE-2015-4703`
`cve: CVE-2015-4704`
`cve: CVE-2015-5468`
`cve: CVE-2015-5469`
`cve: CVE-2015-5471`
`cve: CVE-2015-5472`

... continues on next page ...

... continued from previous page ...

cve: CVE-2015-5609
cve: CVE-2015-9406
cve: CVE-2015-9470
cve: CVE-2015-9480
cve: CVE-2016-10924
cve: CVE-2016-10956
cve: CVE-2017-1002008
cve: CVE-2018-16283
cve: CVE-2018-16299
cve: CVE-2018-7422
cve: CVE-2018-9118
cve: CVE-2019-14205
cve: CVE-2019-14206
cve: CVE-2019-9618
cve: CVE-2020-11738
cve: CVE-2021-39316
cve: CVE-2022-1119
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

High (CVSS: 7.8)
NVT: WordPress Duplicator Plugin < 1.4.7 Information Disclosure Vulnerability

Summary
The WordPress plugin Duplicator is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 1.2.32
Fixed version: 1.4.7
Installation
path / port: /wp-content/plugins/duplicator

Solution:
Solution type: VendorFix
Update to version 1.4.7 or later.

Affected Software/OS
WordPress Duplicator plugin version prior to 1.4.7.

Vulnerability Insight
The Duplicator WordPress plugin discloses the url of the a backup to unauthenticated visitors accessing the main installer endpoint of the plugin, if the installer script has been run once by an administrator, allowing download of the full site backup without authenticating.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: WordPress Duplicator Plugin < 1.4.7 Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.124143
Version used: 2022-08-25T10:12:37Z

References
cve: CVE-2022-2551
url: https://wpscan.com/vulnerability/f27d753e-861a-4d8d-9b9a-6c99a8a7ebe0
url: https://github.com/SecuriTrust/CVEsLab/tree/main/CVE-2022-2551

High (CVSS: 7.5)
NVT: WordPress iThemes Security Plugin < 7.7.0 Incorrect Authorization Vulnerability

Summary
The WordPress plugin 'iThemes Security' enforces authorization rules incorrectly.

Vulnerability Detection Result
Installed version: 7.0.2
Fixed version: 7.7.0
Installation
path / port: /wp-content/plugins/better-wp-security

Impact
If the password requirements are not properly enforced, users may use insecure passwords that can easily be cracked by malicious actors.

Solution:
Solution type: VendorFix
Update to version 7.7.0 or later.

Affected Software/OS
WordPress iThemes Security plugin through version 7.6.1.

Vulnerability Insight
The plugin does not enforce new password requirements on already existing accounts until after the second login.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress iThemes Security Plugin < 7.7.0 Incorrect Authorization Vulnerability
OID:1.3.6.1.4.1.25623.1.0.113811
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2020-36176
url: https://wordpress.org/plugins/better-wp-security/#developers

[return to 172.16.1.7]

2.1.3 Medium 22/tcp

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
```

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: `2022-12-08T10:12:32Z`

. . . continues on next page . . .

... continued from previous page ...

References

```
url: https://weakdh.org/sysadmin.html
url: https://www.rfc-editor.org/rfc/rfc9142.html
url: https://www.rfc-editor.org/rfc/rfc9142.html#name-summary-guidance-for-imple
↪m
url: https://datatracker.ietf.org/doc/html/rfc6194
```

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
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
```

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

... continues on next page ...

... continued from previous page ...

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: `2022-12-09T10:11:04Z`

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

[return to 172.16.1.7]

2.1.4 Medium 443/tcp

Medium (CVSS: 6.5)
NVT: WordPress Elementor Page Builder Plugin <= 2.9.5 Privilege Escalation Vulnerability

Summary
The WordPress plugin 'Elementor Page Builder' is prone to a privilege escalation vulnerability.

Vulnerability Detection Result
```
Installed version: 2.8.5
Fixed version:     2.9.6
Installation
path / port:       /wp-content/plugins/elementor
```

Solution:
Solution type: VendorFix
Update to version 2.9.6 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin through version 2.9.5.

Vulnerability Insight
An authenticated attacker may exploit the safe mode feature to disable all security plugins.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Elementor Page Builder Plugin <= 2.9.5 Privilege Escalation Vulnerabi.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.113750

... continues on next page ...

... continued from previous page ...

Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2020-20634
url: https://blog.nintechnet.com/wordpress-elementor-plugin-fixed-safe-mode-privilege-escalation-vulnerability/

Medium (CVSS: 6.4)
NVT: SSL/TLS: Missing 'secure' Cookie Attribute

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

Vulnerability Detection Result
The cookies:
Set-Cookie: PHPSESSID=***replaced***; path=/
are missing the "secure" attribute.

Solution:
Solution type: Mitigation
Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Affected Software/OS
Server with SSL/TLS.

Vulnerability Insight
The flaw is due to cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks.

Vulnerability Detection Method
Details: SSL/TLS: Missing 'secure' Cookie Attribute
OID:1.3.6.1.4.1.25623.1.0.902661
Version used: 2022-02-15T13:40:32Z

References
url: https://www.owasp.org/index.php/SecureFlag
url: http://www.ietf.org/rfc/rfc2965.txt
url: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

Medium (CVSS: 6.4)
NVT: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.21.83 XSS Vulnerability

Summary
The WordPress plugin 'Anti-Malware Security and Brute-Force Firewall' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 4.18.63
Fixed version:     4.21.83
Installation
path / port:       /wp-content/plugins/gotmls
```

Solution:
Solution type: VendorFix
Update to version 4.21.83 or later.

Affected Software/OS
WordPress Anti-Malware Security and Brute-Force Firewall plugin prior to version 4.21.83.

Vulnerability Insight
The plugin does not sanitise and escape some parameters before outputting them back in an admin dashboard.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.21.83 XSS V.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.127197
Version used: `2022-09-20T10:11:40Z`

References
```
cve: CVE-2022-2599
url: https://wpscan.com/vulnerability/276a7fc5-3d0d-446d-92cf-20060aecd0ef
```

Medium (CVSS: 6.1)
NVT: WordPress Support Plus Responsive Ticket System Plugin < 9.1.2 XSS Vulnerability

Summary
The WordPress plugin 'Support Plus Responsive Ticket System' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 7.1.3
Fixed version:     9.1.2
```

... continues on next page ...

... continued from previous page ...

```
Installation
path / port:        /wp-content/plugins/wp-support-plus-responsive-ticket-system
```

Impact
Successful exploitation would allow an attacker to inject malicious content into an affected site.

Solution:
Solution type: VendorFix
Update to version 9.1.2 or later.

Affected Software/OS
WordPress Support Plus Responsive Ticket System plugin before version 9.1.2.

Vulnerability Detection Method
Details: `WordPress Support Plus Responsive Ticket System Plugin < 9.1.2 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112560
Version used: `2022-07-19T10:11:08Z`

References

```
cve: CVE-2019-7299
url: https://cert.kalasag.com.ph/news/research/cve-2019-7299-stored-xss-in-wp-su
↪pport-plus-responsive-ticket-system/
url: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/#dev
↪elopers
```

Medium (CVSS: 6.1)
NVT: WordPress Photo Gallery Plugin < 1.5.68 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.34
Fixed version:     1.5.68
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.5.68 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.68.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The plugin is vulnerable to reflected XSS issues via the bwg_album_breadcrumb_0 and shortcode_id GET parameters passed to the bwg_frontend_data AJAX action.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.68 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.147922
Version used: `2022-07-19T10:11:08Z`

References
`cve: CVE-2021-25041`
`url: https://wpscan.com/vulnerability/32aee3ea-e0af-44da-a16c-102c83eaed8f`

Medium (CVSS: 6.1)
NVT: WordPress Photo Gallery Plugin < 1.5.69 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.5.69
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.5.69 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.69.

Vulnerability Insight
The WordPress plugin is vulnerable to a reflected XSS issues via the gallery_id, tag, album_id and _id GET parameters passed to the bwg_frontend_data AJAX action (available to both unauthenticated and authenticated users).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.69 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.146158
Version used: `2022-07-19T10:11:08Z`

References

... continues on next page ...

... continued from previous page ...

cve: CVE-2021-24291
url: https://wpscan.com/vulnerability/cfb982b2-8b6d-4345-b3ab-3d2b130b873a
url: https://wordpress.org/plugins/photo-gallery/#developers

Medium (CVSS: 6.1)
NVT: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.20.96 XSS Vulnerability

Summary
The WordPress plugin 'Anti-Malware Security and Brute-Force Firewall' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 4.18.63
Fixed version: 4.20.96
Installation
path / port: /wp-content/plugins/gotmls

Solution:
Solution type: VendorFix
Update to version 4.20.96 or later.

Affected Software/OS
WordPress Anti-Malware Security and Brute-Force Firewall plugin prior to version 4.20.96.

Vulnerability Insight
The plugin does not sanitise and escape the QUERY_STRING before outputting it back in an admin page.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.20.96 XSS V.
↪..
OID:1.3.6.1.4.1.25623.1.0.127196
Version used: 2022-09-20T10:11:40Z

References
cve: CVE-2022-0953
url: https://wpscan.com/vulnerability/29ab3c7b-58e0-4a72-b7b4-ab12a6d54f5a

Medium (CVSS: 6.1)
NVT: WordPress Photo Gallery Plugin < 1.5.75 Multiple Vulnerabilities

Summary

... continues on next page ...

... continued from previous page ...

The WordPress plugin 'Photo Gallery' is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 1.5.34
Fixed version:     1.5.75
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.5.75 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.75.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-24362: The plugin does not ensure that uploaded SVG files added to a gallery do not contain malicious content. As a result, users allowed to add images to gallery can upload an SVG file containing JavaScript code, which will be executed when accessing the image directly (ie in the /wp-content/uploads/photo-gallery/ folder), leading to a Cross-Site Scripting (XSS) issue.
- CVE-2021-24363: The plugin does not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images/SVG anywhere in the filesystem via a path traversal vector.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.75 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.146543
Version used: `2022-07-19T10:11:08Z`

References

```
cve: CVE-2021-24362
cve: CVE-2021-24363
url: https://wpscan.com/vulnerability/57823dcb-2149-47f7-aae2-d9f04dce851a
url: https://wpscan.com/vulnerability/1628935f-1d7d-4609-b7a9-e5526499c974
url: https://wordpress.org/plugins/photo-gallery/#developers
```

Medium (CVSS: 6.1)
NVT: WordPress Elementor Page Builder Plugin <= 3.5.5 XSS Vulnerability

Summary
The WordPress plugin 'Elementor Page Builder' is prone to a cross-site scripting (XSS) vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 2.8.5
Fixed version: 3.5.6
Installation
path / port: /wp-content/plugins/elementor

Impact
An attacker could do the following: account takeovers, executing javascript on victim's behalf, SOAP bypass, CORS bypass, Defacement.

Solution:
Solution type: VendorFix
Update to version 3.5.6 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin version 3.5.5 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Elementor Page Builder Plugin <= 3.5.5 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.126057
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2022-29455
url: https://patchstack.com/database/vulnerability/elementor/wordpress-elementor-plugin-3-5-5-unauthenticated-dom-based-reflected-cross-site-scripting-xss-vulnerability
url: https://rotem-bar.com/hacking-65-million-websites-greater-cve-2022-29455-elementor
url: https://www.wordfence.com/blog/2022/04/elementor-critical-remote-code-execution-vulnerability/

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
The web server has the following HTTP methods enabled: TRACE

Impact

... continues on next page ...

... continued from previous page ...

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2022-05-12T09:32:01Z`

References
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`
`cve: CVE-2014-7883`
`url: http://www.kb.cert.org/vuls/id/288308`
`url: http://www.securityfocus.com/bid/11604`
`url: http://www.securityfocus.com/bid/15222`
`url: http://www.securityfocus.com/bid/19915`
`url: http://www.securityfocus.com/bid/24456`
`url: http://www.securityfocus.com/bid/33374`
`url: http://www.securityfocus.com/bid/36956`
`url: http://www.securityfocus.com/bid/36990`
`url: http://www.securityfocus.com/bid/37995`
`url: http://www.securityfocus.com/bid/9506`
`url: http://www.securityfocus.com/bid/9561`
`url: http://www.kb.cert.org/vuls/id/867593`
`url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable`

... continues on next page ...

... continued from previous page ...

url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020

Medium (CVSS: 5.5)
NVT: WordPress Elementor Page Builder Plugin <= 3.1.1 Multiple XSS Vulnerabilities

Summary
The WordPress plugin 'Elementor Page Builder' is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result
Installed version: 2.8.5
Fixed version: 3.1.4
Installation
path / port: /wp-content/plugins/elementor

Solution:
Solution type: VendorFix
Update to version 3.1.4 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin through version 3.1.1.

Vulnerability Insight
Multiple stored XSS vulnerabilities are present in Elementor, which could be exploited via the Column element as well as the Accordion, Icon Box, Image Box, Heading, and Divider components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Elementor Page Builder Plugin <= 3.1.1 Multiple XSS Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.145596
Version used: 2022-07-19T10:11:08Z

References
url: https://wordpress.org/plugins/elementor/#developers
url: https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities
↪-in-elementor-impact-over-7-million-sites/

Medium (CVSS: 5.4)
NVT: WordPress Elementor Page Builder Plugin <= 2.9.13 XSS Vulnerability

Summary
The WordPress plugin 'Elementor Page Builder' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 2.8.5
Fixed version:     2.9.14
Installation
path / port:       /wp-content/plugins/elementor
```

Impact
Successful exploitation would allow an attacker to inject arbitrary HTML and JavaScript into the page.

Solution:
Solution type: VendorFix
Update to version 2.9.14 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin through version 2.9.13.

Vulnerability Insight
The vulnerability is exploitable via the Name Your Template field.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Elementor Page Builder Plugin <= 2.9.13 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113751
Version used: `2022-07-19T10:11:08Z`

References
```
cve: CVE-2020-15020
url: http://hidden-one.co.in/2020/07/07/cve-2020-1020-stored-xss-on-elementor-wo
↪rdpress-plugin/
```

Medium (CVSS: 5.4)
NVT: WordPress Elementor Page Builder Plugin < 2.9.9 Multiple XSS Vulnerabilities

Summary
The WordPress plugin 'Elementor Page Builder' is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Installed version: 2.8.5
Fixed version: 2.9.9
Installation
path / port: /wp-content/plugins/elementor

Impact
Successful exploitation would allow an authenticated attacker to inject arbitrary HTML or JavaScript into the site.

Solution:
Solution type: VendorFix
Update to version 2.9.9 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin before version 2.9.9.

Vulnerability Insight
An author user can create posts that result in stored XSS by using a crafted payload in custom links, using a crafted link in the custom URL or by applying custom attributes.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Elementor Page Builder Plugin < 2.9.9 Multiple XSS Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.112765
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2020-13864
cve: CVE-2020-13865
url: https://wordpress.org/plugins/elementor/#developers
url: https://www.softwaresecured.com/elementor-page-builder-stored-xss/

Medium (CVSS: 5.4)
NVT: WordPress WPForms Contact Form Plugin < 1.5.9 XSS Vulnerability

Summary
The WordPress plugin 'WPForms Contact Form' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 1.5.8.2
Fixed version: 1.5.9
Installation
path / port: /wp-content/plugins/wpforms-lite

... continues on next page ...

... continued from previous page ...

Impact
Successful exploitation would allow an authenticated attacker to inject arbitrary HTML and JavaScript into the site.

Solution:
Solution type: VendorFix
Update to version 1.5.9 or later.

Affected Software/OS
WordPress WPForms Contact Form plugin through version 1.5.8.2.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress WPForms Contact Form Plugin < 1.5.9 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113660
Version used: `2022-07-19T10:11:08Z`

References
```
cve: CVE-2020-10385
url: https://wordpress.org/plugins/wpforms-lite/#developers
url: https://www.getastra.com/blog/911/plugin-exploit/stored-xss-vulnerability-f
↪ound-in-wpforms-plugin/
url: https://www.jinsonvarghese.com/stored-xss-vulnerability-found-in-wpforms-pl
↪ugin/
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result
```
The certificate of the remote service expired on 2021-01-29 18:25:03.
Certificate details:
fingerprint (SHA-1)                | 215634A02F827BD6CC5C43526063125B37BBF046
fingerprint (SHA-256)              | F3437F6D633DB628134A8B0D501B5BA3D3D7F9161D49AA
↪3BD88A9D81F042DD2D
issued by                          | 1.2.840.113549.1.9.1=#696E666F4061726D6F757269
↪6E666F7365632E636F6D,CN=armour infosec,OU=IT,O=Armour infosec,L=indore,ST=MP,C
↪=IN
public key algorithm               | RSA
public key size (bits)             | 2048
serial                             | 00CFC6A4E59988DF9D
signature algorithm                | sha256WithRSAEncryption
subject                            | 1.2.840.113549.1.9.1=#696E666F4061726D6F757269
↪6E666F7365632E636F6D,CN=armour infosec,OU=IT,O=Armour infosec,L=indore,ST=MP,C
```

... continues on next page ...

... continued from previous page ...

```
↪=IN
subject alternative names (SAN) | None
valid from                      | 2020-01-30 18:25:03 UTC
valid until                     | 2021-01-29 18:25:03 UTC
```

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `2021-11-22T15:32:39Z`

Medium (CVSS: 5.0)
NVT: Missing 'httpOnly' Cookie Attribute

Summary
The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result

```
The cookies:
Set-Cookie: PHPSESSID=***replaced***; path=/
are missing the "httpOnly" attribute.
```

Solution:
Solution type: Mitigation
Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS
Application with session handling in cookies.

Vulnerability Insight
The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Check all cookies sent by the application for a missing 'httpOnly' attribute
Details: `Missing 'httpOnly' Cookie Attribute`
OID:1.3.6.1.4.1.25623.1.0.105925

... continues on next page ...

... continued from previous page ...

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

References
url: https://www.owasp.org/index.php/HttpOnly
url: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

Medium (CVSS: 5.0)
NVT: WordPress Duplicator Plugin < 1.4.7.1 Information Disclosure Vulnerability

Summary
The WordPress plugin 'Duplicator' is prone to an information disclosure vulnerability.

Vulnerability Detection Result
Installed version: 1.2.32
Fixed version: 1.4.7.1
Installation
path / port: /wp-content/plugins/duplicator

Solution:
Solution type: VendorFix
Update to version 1.4.7.1 or later.

Affected Software/OS
WordPress Duplicator plugin version prior to 1.4.7.1.

Vulnerability Insight
The Duplicator WordPress plugin does not authenticate or authorize visitors before displaying information about the system such as server software, php version and full file system path to the site.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Duplicator Plugin < 1.4.7.1 Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.124142
Version used: 2022-08-25T10:12:37Z

References
cve: CVE-2022-2552
url: https://wpscan.com/vulnerability/6b540712-fda5-4be6-ae4b-bd30a9d9d698
url: https://github.com/SecuriTrust/CVEsLab/tree/main/CVE-2022-2552

Medium (CVSS: 4.8)
NVT: WordPress Photo Gallery Plugin < 1.5.46 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.5.46
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Impact
Successful exploitation of this vulnerability would allow an authenticated admin user to inject arbitrary JavaScript code that is viewed by other users.

Solution:
Solution type: VendorFix
Update to version 1.5.46 or later.

Affected Software/OS
WordPress Photo Gallery plugin before 1.5.46.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.46 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112708
Version used: `2022-07-19T10:11:08Z`

References
```
cve: CVE-2020-9335
url: https://wpvulndb.com/vulnerabilities/10088
url: https://wordpress.org/plugins/photo-gallery/#developers
```

Medium (CVSS: 4.8)
NVT: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.20.94 XSS Vulnerability

Summary
The WordPress plugin 'Anti-Malware Security and Brute-Force Firewall' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 4.18.63
Fixed version:     4.20.94
Installation
```

... continues on next page ...

... continued from previous page ...

path / port: /wp-content/plugins/gotmls

Solution:
Solution type: VendorFix
Update to version 4.20.94 or later.

Affected Software/OS
WordPress Anti-Malware Security and Brute-Force Firewall plugin prior to version 4.20.94.

Vulnerability Insight
The plugin does not sanitise and escape the POST data before outputting it back in attributes of an admin page, leading to a reflected XSS. Due to the presence of specific parameter value, available to admin users, this can only be exploited by an admin against another admin user.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.20.94 XSS V.
↪..
OID:1.3.6.1.4.1.25623.1.0.147732
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2021-25101
url: https://wpscan.com/vulnerability/5fd0380c-0d1d-4380-96f0-a07be5a61eba

Medium (CVSS: 4.8)
NVT: WordPress Photo Gallery Plugin < 1.5.67 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 1.5.34
Fixed version: 1.5.67
Installation
path / port: /wp-content/plugins/photo-gallery

Solution:
Solution type: VendorFix
Update to version 1.5.67 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.67.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The WordPress plugin does not properly sanitise the gallery title, allowing high privilege users to create one with XSS payload in it, which will be triggered when another user will view the gallery list or the affected gallery in the admin dashboard. This is due to an incomplete fix of CVE-2019-16117.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.67 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.146159
Version used: `2022-07-19T10:11:08Z`

References
`cve: CVE-2021-24310`
`url: https://wpscan.com/vulnerability/f34096ec-b1b0-471d-88a4-4699178a3165`
`url: https://wordpress.org/plugins/photo-gallery/#developers`

Medium (CVSS: 4.8)
NVT: WordPress Photo Gallery Plugin < 1.6.4 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.6.4
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.6.4 or later.

Affected Software/OS
WordPress Photo Gallery plugin prior to version 1.6.4.

Vulnerability Insight
The plugin does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.6.4 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.124080

... continues on next page ...

... continued from previous page ...

Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2022-1394
url: https://wpscan.com/vulnerability/f7a0df37-3204-4926-84ec-2204a2f22de3

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

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[return to 172.16.1.7]

2.1.5 Medium 80/tcp

Medium (CVSS: 6.5)
NVT: WordPress Elementor Page Builder Plugin <= 2.9.5 Privilege Escalation Vulnerability

Summary
The WordPress plugin 'Elementor Page Builder' is prone to a privilege escalation vulnerability.

Vulnerability Detection Result

```
Installed version: 2.8.5
Fixed version:     2.9.6
Installation
path / port:       /wp-content/plugins/elementor
```

Solution:
Solution type: VendorFix
Update to version 2.9.6 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin through version 2.9.5.

Vulnerability Insight
An authenticated attacker may exploit the safe mode feature to disable all security plugins.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: WordPress Elementor Page Builder Plugin <= 2.9.5 Privilege Escalation Vulnerabi.
↪..
OID:1.3.6.1.4.1.25623.1.0.113750
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2020-20634
url: https://blog.nintechnet.com/wordpress-elementor-plugin-fixed-safe-mode-priv
↪ilege-escalation-vulnerability/

Medium (CVSS: 6.4)
NVT: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.21.83 XSS Vulnerability

Summary
The WordPress plugin 'Anti-Malware Security and Brute-Force Firewall' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 4.18.63
Fixed version: 4.21.83
Installation
path / port: /wp-content/plugins/gotmls

Solution:
Solution type: VendorFix
Update to version 4.21.83 or later.

Affected Software/OS
WordPress Anti-Malware Security and Brute-Force Firewall plugin prior to version 4.21.83.

Vulnerability Insight
The plugin does not sanitise and escape some parameters before outputting them back in an admin dashboard.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.21.83 XSS V.
↪..
OID:1.3.6.1.4.1.25623.1.0.127197
Version used: 2022-09-20T10:11:40Z

References
cve: CVE-2022-2599
url: https://wpscan.com/vulnerability/276a7fc5-3d0d-446d-92cf-20060aecd0ef

Medium (CVSS: 6.1)
NVT: WordPress Photo Gallery Plugin < 1.5.68 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.5.68
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.5.68 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.68.

Vulnerability Insight
The plugin is vulnerable to reflected XSS issues via the bwg_album_breadcrumb_0 and shortcode_id GET parameters passed to the bwg_frontend_data AJAX action.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.68 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.147922
Version used: `2022-07-19T10:11:08Z`

References
```
cve: CVE-2021-25041
url: https://wpscan.com/vulnerability/32aee3ea-e0af-44da-a16c-102c83eaed8f
```

Medium (CVSS: 6.1)
NVT: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.20.96 XSS Vulnerability

Summary
The WordPress plugin 'Anti-Malware Security and Brute-Force Firewall' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 4.18.63
Fixed version:     4.20.96
Installation
path / port:       /wp-content/plugins/gotmls
```

... continues on next page ...

... continued from previous page ...

Solution:
Solution type: VendorFix
Update to version 4.20.96 or later.

Affected Software/OS
WordPress Anti-Malware Security and Brute-Force Firewall plugin prior to version 4.20.96.

Vulnerability Insight
The plugin does not sanitise and escape the QUERY_STRING before outputting it back in an admin page.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.20.96 XSS V.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.127196
Version used: `2022-09-20T10:11:40Z`

References
`cve: CVE-2022-0953`
`url: https://wpscan.com/vulnerability/29ab3c7b-58e0-4a72-b7b4-ab12a6d54f5a`

Medium (CVSS: 6.1)
NVT: WordPress Support Plus Responsive Ticket System Plugin < 9.1.2 XSS Vulnerability

Summary
The WordPress plugin 'Support Plus Responsive Ticket System' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 7.1.3
Fixed version:     9.1.2
Installation
path / port:       /wp-content/plugins/wp-support-plus-responsive-ticket-system
```

Impact
Successful exploitation would allow an attacker to inject malicious content into an affected site.

Solution:
Solution type: VendorFix
Update to version 9.1.2 or later.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

WordPress Support Plus Responsive Ticket System plugin before version 9.1.2.

Vulnerability Detection Method
Details: `WordPress Support Plus Responsive Ticket System Plugin < 9.1.2 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112560
Version used: `2022-07-19T10:11:08Z`

References
`cve: CVE-2019-7299`
`url: https://cert.kalasag.com.ph/news/research/cve-2019-7299-stored-xss-in-wp-su`
`↪pport-plus-responsive-ticket-system/`
`url: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/#dev`
`↪elopers`

Medium (CVSS: 6.1)
NVT: WordPress Elementor Page Builder Plugin <= 3.5.5 XSS Vulnerability

Summary
The WordPress plugin 'Elementor Page Builder' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 2.8.5
Fixed version:     3.5.6
Installation
path / port:       /wp-content/plugins/elementor
```

Impact
An attacker could do the following: account takeovers, executing javascript on victim's behalf, SOAP bypass, CORS bypass, Defacement.

Solution:
Solution type: VendorFix
Update to version 3.5.6 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin version 3.5.5 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Elementor Page Builder Plugin <= 3.5.5 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.126057
Version used: `2022-07-19T10:11:08Z`

References

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-29455
url: https://patchstack.com/database/vulnerability/elementor/wordpress-elementor-plugin-3-5-5-unauthenticated-dom-based-reflected-cross-site-scripting-xss-vulnerability
url: https://rotem-bar.com/hacking-65-million-websites-greater-cve-2022-29455-elementor
url: https://www.wordfence.com/blog/2022/04/elementor-critical-remote-code-execution-vulnerability/

Medium (CVSS: 6.1)
NVT: WordPress Photo Gallery Plugin < 1.5.69 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 1.5.34
Fixed version: 1.5.69
Installation
path / port: /wp-content/plugins/photo-gallery

Solution:
Solution type: VendorFix
Update to version 1.5.69 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.69.

Vulnerability Insight
The WordPress plugin is vulnerable to a reflected XSS issues via the gallery_id, tag, album_id and _id GET parameters passed to the bwg_frontend_data AJAX action (available to both unauthenticated and authenticated users).

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Photo Gallery Plugin < 1.5.69 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.146158
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2021-24291
url: https://wpscan.com/vulnerability/cfb982b2-8b6d-4345-b3ab-3d2b130b873a
url: https://wordpress.org/plugins/photo-gallery/#developers

Medium (CVSS: 6.1)
NVT: WordPress Photo Gallery Plugin < 1.5.75 Multiple Vulnerabilities

Summary
The WordPress plugin 'Photo Gallery' is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.5.75
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.5.75 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.75.

Vulnerability Insight
The following vulnerabilities exist:
- CVE-2021-24362: The plugin does not ensure that uploaded SVG files added to a gallery do not contain malicious content. As a result, users allowed to add images to gallery can upload an SVG file containing JavaScript code, which will be executed when accessing the image directly (ie in the /wp-content/uploads/photo-gallery/ folder), leading to a Cross-Site Scripting (XSS) issue.
- CVE-2021-24363: The plugin does not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images/SVG anywhere in the filesystem via a path traversal vector.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.75 Multiple Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.146543
Version used: `2022-07-19T10:11:08Z`

References
```
cve: CVE-2021-24362
cve: CVE-2021-24363
url: https://wpscan.com/vulnerability/57823dcb-2149-47f7-aae2-d9f04dce851a
url: https://wpscan.com/vulnerability/1628935f-1d7d-4609-b7a9-e5526499c974
url: https://wordpress.org/plugins/photo-gallery/#developers
```

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

... continues on next page ...

... continued from previous page ...

Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2022-05-12T09:32:01Z`

References
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`
`cve: CVE-2014-7883`
`url: http://www.kb.cert.org/vuls/id/288308`
`url: http://www.securityfocus.com/bid/11604`
`url: http://www.securityfocus.com/bid/15222`
`url: http://www.securityfocus.com/bid/19915`
`url: http://www.securityfocus.com/bid/24456`

... continues on next page ...

... continued from previous page ...

```
url: http://www.securityfocus.com/bid/33374
url: http://www.securityfocus.com/bid/36956
url: http://www.securityfocus.com/bid/36990
url: http://www.securityfocus.com/bid/37995
url: http://www.securityfocus.com/bid/9506
url: http://www.securityfocus.com/bid/9561
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac
↪e-verbs/ba-p/784482
url: https://owasp.org/www-community/attacks/Cross_Site_Tracing
cert-bund: CB-K14/0981
dfn-cert: DFN-CERT-2021-1825
dfn-cert: DFN-CERT-2014-1018
dfn-cert: DFN-CERT-2010-0020
```

Medium (CVSS: 5.5)
NVT: WordPress Elementor Page Builder Plugin <= 3.1.1 Multiple XSS Vulnerabilities

Summary
The WordPress plugin 'Elementor Page Builder' is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result

```
Installed version: 2.8.5
Fixed version:     3.1.4
Installation
path / port:       /wp-content/plugins/elementor
```

Solution:
Solution type: VendorFix
Update to version 3.1.4 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin through version 3.1.1.

Vulnerability Insight
Multiple stored XSS vulnerabilities are present in Elementor, which could be exploited via the Column element as well as the Accordion, Icon Box, Image Box, Heading, and Divider components.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Elementor Page Builder Plugin <= 3.1.1 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.145596

... continues on next page ...

... continued from previous page ...

Version used: 2022-07-19T10:11:08Z

References
url: https://wordpress.org/plugins/elementor/#developers
url: https://www.wordfence.com/blog/2021/03/cross-site-scripting-vulnerabilities-in-elementor-impact-over-7-million-sites/

Medium (CVSS: 5.4)
NVT: WordPress Elementor Page Builder Plugin < 2.9.9 Multiple XSS Vulnerabilities

Summary
The WordPress plugin 'Elementor Page Builder' is prone to multiple cross-site scripting (XSS) vulnerabilities.

Vulnerability Detection Result
Installed version: 2.8.5
Fixed version: 2.9.9
Installation
path / port: /wp-content/plugins/elementor

Impact
Successful exploitation would allow an authenticated attacker to inject arbitrary HTML or JavaScript into the site.

Solution:
Solution type: VendorFix
Update to version 2.9.9 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin before version 2.9.9.

Vulnerability Insight
An author user can create posts that result in stored XSS by using a crafted payload in custom links, using a crafted link in the custom URL or by applying custom attributes.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Elementor Page Builder Plugin < 2.9.9 Multiple XSS Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.112765
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2020-13864
cve: CVE-2020-13865
url: https://wordpress.org/plugins/elementor/#developers
url: https://www.softwaresecured.com/elementor-page-builder-stored-xss/

Medium (CVSS: 5.4)
NVT: WordPress Elementor Page Builder Plugin <= 2.9.13 XSS Vulnerability

Summary
The WordPress plugin 'Elementor Page Builder' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 2.8.5
Fixed version:     2.9.14
Installation
path / port:       /wp-content/plugins/elementor
```

Impact
Successful exploitation would allow an attacker to inject arbitrary HTML and JavaScript into the page.

Solution:
Solution type: VendorFix
Update to version 2.9.14 or later.

Affected Software/OS
WordPress Elementor Page Builder plugin through version 2.9.13.

Vulnerability Insight
The vulnerability is exploitable via the Name Your Template field.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Elementor Page Builder Plugin <= 2.9.13 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113751
Version used: `2022-07-19T10:11:08Z`

References
```
cve: CVE-2020-15020
url: http://hidden-one.co.in/2020/07/07/cve-2020-1020-stored-xss-on-elementor-wo
↪rdpress-plugin/
```

Medium (CVSS: 5.4)
NVT: WordPress WPForms Contact Form Plugin < 1.5.9 XSS Vulnerability

Summary
The WordPress plugin 'WPForms Contact Form' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

```
Installed version: 1.5.8.2
Fixed version:     1.5.9
Installation
path / port:       /wp-content/plugins/wpforms-lite
```

Impact
Successful exploitation would allow an authenticated attacker to inject arbitrary HTML and JavaScript into the site.

Solution:
Solution type: VendorFix
Update to version 1.5.9 or later.

Affected Software/OS
WordPress WPForms Contact Form plugin through version 1.5.8.2.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress WPForms Contact Form Plugin < 1.5.9 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113660
Version used: `2022-07-19T10:11:08Z`

References

```
cve: CVE-2020-10385
url: https://wordpress.org/plugins/wpforms-lite/#developers
url: https://www.getastra.com/blog/911/plugin-exploit/stored-xss-vulnerability-f
↪ound-in-wpforms-plugin/
url: https://www.jinsonvarghese.com/stored-xss-vulnerability-found-in-wpforms-pl
↪ugin/
```

Medium (CVSS: 5.0)
NVT: Missing 'httpOnly' Cookie Attribute

Summary
The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result

```
The cookies:
Set-Cookie: PHPSESSID=***replaced***; path=/
are missing the "httpOnly" attribute.
```

Solution:
Solution type: Mitigation
Set the 'httpOnly' attribute for any session cookie.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Application with session handling in cookies.

Vulnerability Insight
The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Check all cookies sent by the application for a missing 'httpOnly' attribute
Details: `Missing 'httpOnly' Cookie Attribute`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2020-08-24T15:18:35Z`

References
`url: https://www.owasp.org/index.php/HttpOnly`
`url: https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-00`
`↪2)`

Medium (CVSS: 5.0)
NVT: WordPress Duplicator Plugin < 1.4.7.1 Information Disclosure Vulnerability

Summary
The WordPress plugin 'Duplicator' is prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 1.2.32
Fixed version:     1.4.7.1
Installation
path / port:       /wp-content/plugins/duplicator
```

Solution:
Solution type: VendorFix
Update to version 1.4.7.1 or later.

Affected Software/OS
WordPress Duplicator plugin version prior to 1.4.7.1.

Vulnerability Insight
The Duplicator WordPress plugin does not authenticate or authorize visitors before displaying information about the system such as server software, php version and full file system path to the site.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: WordPress Duplicator Plugin < 1.4.7.1 Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.124142
Version used: 2022-08-25T10:12:37Z

References
cve: CVE-2022-2552
url: https://wpscan.com/vulnerability/6b540712-fda5-4be6-ae4b-bd30a9d9d698
url: https://github.com/SecuriTrust/CVEsLab/tree/main/CVE-2022-2552

Medium (CVSS: 4.8)
NVT: WordPress Photo Gallery Plugin < 1.5.67 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
Installed version: 1.5.34
Fixed version: 1.5.67
Installation
path / port: /wp-content/plugins/photo-gallery

Solution:
Solution type: VendorFix
Update to version 1.5.67 or later.

Affected Software/OS
WordPress Photo Gallery plugin before version 1.5.67.

Vulnerability Insight
The WordPress plugin does not properly sanitise the gallery title, allowing high privilege users to create one with XSS payload in it, which will be triggered when another user will view the gallery list or the affected gallery in the admin dashboard. This is due to an incomplete fix of CVE-2019-16117.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: WordPress Photo Gallery Plugin < 1.5.67 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.146159
Version used: 2022-07-19T10:11:08Z

References
cve: CVE-2021-24310
url: https://wpscan.com/vulnerability/f34096ec-b1b0-471d-88a4-4699178a3165
url: https://wordpress.org/plugins/photo-gallery/#developers

Medium (CVSS: 4.8)
NVT: WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.20.94 XSS Vulnerability

Summary
The WordPress plugin 'Anti-Malware Security and Brute-Force Firewall' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 4.18.63
Fixed version:     4.20.94
Installation
path / port:       /wp-content/plugins/gotmls
```

Solution:
Solution type: VendorFix
Update to version 4.20.94 or later.

Affected Software/OS
WordPress Anti-Malware Security and Brute-Force Firewall plugin prior to version 4.20.94.

Vulnerability Insight
The plugin does not sanitise and escape the POST data before outputting it back in attributes of an admin page, leading to a reflected XSS. Due to the presence of specific parameter value, available to admin users, this can only be exploited by an admin against another admin user.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Anti-Malware Security and Brute-Force Firewall Plugin < 4.20.94 XSS V.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.147732
Version used: `2022-07-19T10:11:08Z`

References
```
cve: CVE-2021-25101
url: https://wpscan.com/vulnerability/5fd0380c-0d1d-4380-96f0-a07be5a61eba
```

Medium (CVSS: 4.8)
NVT: WordPress Photo Gallery Plugin < 1.5.46 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result
```
Installed version: 1.5.34
Fixed version:     1.5.46
```

... continues on next page ...

... continued from previous page ...

```
Installation
path / port:        /wp-content/plugins/photo-gallery
```

Impact
Successful exploitation of this vulnerability would allow an authenticated admin user to inject arbitrary JavaScript code that is viewed by other users.

Solution:
Solution type: VendorFix
Update to version 1.5.46 or later.

Affected Software/OS
WordPress Photo Gallery plugin before 1.5.46.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.5.46 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112708
Version used: `2022-07-19T10:11:08Z`

References
`cve: CVE-2020-9335`
`url: https://wpvulndb.com/vulnerabilities/10088`
`url: https://wordpress.org/plugins/photo-gallery/#developers`

Medium (CVSS: 4.8)
NVT: WordPress Photo Gallery Plugin < 1.6.4 XSS Vulnerability

Summary
The WordPress plugin 'Photo Gallery' is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 1.5.34
Fixed version:     1.6.4
Installation
path / port:       /wp-content/plugins/photo-gallery
```

Solution:
Solution type: VendorFix
Update to version 1.6.4 or later.

Affected Software/OS
WordPress Photo Gallery plugin prior to version 1.6.4.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The plugin does not properly validate and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks when unfiltered_html is disallowed

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress Photo Gallery Plugin < 1.6.4 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.124080
Version used: `2022-07-19T10:11:08Z`

References
`cve: CVE-2022-1394`
`url: https://wpscan.com/vulnerability/f7a0df37-3204-4926-84ec-2204a2f22de3`

[return to 172.16.1.7]

2.1.6 Low general/icmp

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

Summary
The remote host responded to an ICMP timestamp request.

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

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

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

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

... continues on next page ...

... continued from previous page ...

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

[return to 172.16.1.7]

2.1.7 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 4294939245
Packet 2: 4294940442

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

... continues on next page ...

... continued from previous page ...

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

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

[return to 172.16.1.7]