Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Vulnerability Assessment of the STAFF server ICAR-CNR sede Rende

Sabrina Celia, Danilo Cistaro

RT-ICAR-CS-22-04 **Febbraio 2022**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 8-9C, 87036 Rende, Italy, URL: www.icar.cnr.it
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: www.icar.cnr.it
– Sezione di Palermo, Via Ugo La Malfa, 153, 90146 Palermo, URL: www.icar.cnr.it

Introduction

Vulnerability scanners are essential and precious tools that search for and report on known vulnerabilities in an organisation's IT infrastructure. Using a vulnerability scanner is a simple but essential security practice that any organisation can benefit from. These scans can give an organisation an idea of the security threats it may face, providing insight into potential security weaknesses in their systems.

Many organisations use multiple vulnerability scanners to ensure that they have complete coverage and protection of the entire organisation. Over the years, many scanners have been developed, offering many options and different functionalities; as far as our research institute is concerned, given the type of data that can be exposed to possible attacks by hackers, we preferred to assess the risk of vulnerabilities through the OpenVAS tool; the tool is supported by a database of vulnerabilities, this database is used by the scanner to analyse any possible criticality whenever it finds a service listening. The scanning tool receives daily updates from the Network Vulnerability Tests 'NVTs' database.

The personal websites of ICAR-CNR employees are published on the Institute Staff site. The site is intended to publicise the CVs and experience of individual employees on the Internet. Each employee has the possibility of publishing personal pages using the numerous web technologies available.

The ICAR-CNR staff site is available at http://staff.icar.cnr.it , the report generated after the scan shows that the main vulnerabilities are attributable to the Wordpress sites installed in the personal pages of individual users. In order to increase the level of security, we recommend updating the Wordpress versions of the personal sites used by users.

Scan Report

January 25, 2022

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 150.145.63.3". The scan started at Tue Jan 25 15:23:50 2022 UTC and ended at Tue Jan 25 16:38:33 2022 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
150.145.63.3 staff.icar.cnr.it	2	24	1	0	0
Total: 1	2	24	1	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 27 results selected by the filtering described above. Before filtering there were 261 results.

2 Results per Host

2.1 150.145.63.3

Host scan start	Tue Jan 25 15:24:36 2022 UTC
Host scan end	Tue Jan 25 16:38:27 2022 UTC

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

2.1.1 High 443/tcp

High (CVSS: 10.0)
NVT: WordPress Contact Form 7 Plugin < 5.3.2 RCE Vulnerability

Summary
WordPress Contact Form 7 plugin is prone to an unrestricted file upload and remote code execution vulnerability because a filename may contain special characters.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
Installed version: 5.1.8
Fixed version:     5.3.2
Installation
path / port:       /costa/wordpress/wp-content/plugins/contact-form-7
```

Impact

Attackers may upload files of any type, bypassing all restrictions placed regarding the allowed upload-able file types on a website. Further, it allows an attacker to inject malicious content such as web shells.

Solution:

Solution type: VendorFix

Update to version 5.3.2 or later.

Affected Software/OS

WordPress Contact Form 7 plugin version 5.3.1 and prior.

Vulnerability Detection Method

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

Details: `WordPress Contact Form 7 Plugin < 5.3.2 RCE Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.145080

Version used: `2021-07-07T02:00:46Z`

References

```
cve: CVE-2020-35489
url: https://contactform7.com/2020/12/17/contact-form-7-532/
url: https://www.getastra.com/blog/911/plugin-exploit/contact-form-7-unrestricte
↪d-file-upload/
url: https://www.jinsonvarghese.com/unrestricted-file-upload-in-contact-form-7/
```

[return to 150.145.63.3]

2.1.2 High 80/tcp

High (CVSS: 10.0)

NVT: WordPress Contact Form 7 Plugin < 5.3.2 RCE Vulnerability

Summary

WordPress Contact Form 7 plugin is prone to an unrestricted file upload and remote code execution vulnerability because a filename may contain special characters.

Vulnerability Detection Result

```
Installed version: 5.1.8
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     5.3.2
Installation
path / port:       /costa/wordpress/wp-content/plugins/contact-form-7
```

Impact

Attackers may upload files of any type, bypassing all restrictions placed regarding the allowed upload-able file types on a website. Further, it allows an attacker to inject malicious content such as web shells.

Solution:

Solution type: VendorFix

Update to version 5.3.2 or later.

Affected Software/OS

WordPress Contact Form 7 plugin version 5.3.1 and prior.

Vulnerability Detection Method

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

Details: `WordPress Contact Form 7 Plugin < 5.3.2 RCE Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.145080

Version used: `2021-07-07T02:00:46Z`

References

```
cve: CVE-2020-35489
url: https://contactform7.com/2020/12/17/contact-form-7-532/
url: https://www.getastra.com/blog/911/plugin-exploit/contact-form-7-unrestricte
↪d-file-upload/
url: https://www.jinsonvarghese.com/unrestricted-file-upload-in-contact-form-7/
```

[return to 150.145.63.3]

2.1.3 Medium 443/tcp

Medium (CVSS: 6.8)

NVT: WordPress TablePress Plugin < 1.10 CSV Injection Vulnerability

Summary

The WordPress plugin TablePress is prone to a CSV injection vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.2
Fixed version:     1.10
Installation
path / port:       /costa/wordpress/wp-content/plugins/tablepress
```

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation would allow an attacker to force an unknown user to execute code on the affected device.

Solution:
Solution type: VendorFix
Update to version 1.10 or later.

Affected Software/OS
WordPress TablePress plugin before version 1.10.

Vulnerability Detection Method
Details: `WordPress TablePress Plugin < 1.10 CSV Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112685
Version used: `2021-07-07T02:00:46Z`

References

```
cve: CVE-2019-20180
url: https://wordpress.org/plugins/tablepress/#developers
url: https://medium.com/@Pablo0xSantiago/cve-2019-20180-tablepress-version-1-9-2
↪-csv-injection-65309fcc8be8
```

Medium (CVSS: 6.1)
NVT: WordPress All In One WP Security & Firewall Plugin < 4.4.6 XSS Vulnerability

Summary
The WordPress plugin All In One WP Security & Firewall is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     4.4.6
Installation
path / port:       /costa/wordpress/wp-content/plugins/all-in-one-wp-security-an
↪d-firewall
```

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

Solution:
Solution type: VendorFix
Update to version 4.4.6.

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS
WordPress All In One WP Security & Firewall plugin through 4.4.5.

Vulnerability Insight
The vulnerability is exploitable via the wp-security-blacklist-menu.php page.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress All In One WP Security & Firewall Plugin < 4.4.6 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113788
Version used: `2021-08-17T12:00:57Z`

References
```
cve: CVE-2020-29171
url: https://github.com/Arsenal21/all-in-one-wordpress-security/commit/4130906bc
↪049b195467b4fc6980d6d304fbe28d5
url: https://wordpress.org/plugins/all-in-one-wp-security-and-firewall
```

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
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.

. . . continues on next page . . .

. . . continued from previous page . . .

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: `2021-02-15T07:14:40Z`

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
bid: 9506
bid: 9561
bid: 11604
bid: 15222
bid: 19915
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
url: http://www.kb.cert.org/vuls/id/288308
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: 5.4)
NVT: WordPress Google Maps Plugin < 8.1.13 XSS Vulnerability

Summary

The WordPress plugin Google Maps is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.25
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Fixed version:     8.1.13
Installation
path / port:       /costa/wordpress/wp-content/plugins/wp-google-maps
```

Solution:
Solution type: VendorFix
Update to version 8.1.13 or later.

Affected Software/OS
WordPress Google Maps plugin version 8.1.12 and prior.

Vulnerability Detection Method
Details: `WordPress Google Maps Plugin < 8.1.13 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.146812
Version used: `2021-09-30T13:01:29Z`

References

```
cve: CVE-2021-36870
url: https://patchstack.com/database/vulnerability/wp-google-maps/wordpress-wp-g
↪oogle-maps-plugin-8-1-12-multiple-authenticated-persistent-cross-site-scriptin
↪g-xss-vulnerabilities
url: https://wordpress.org/plugins/wp-google-maps/#developers
```

Medium (CVSS: 5.4)
NVT: WordPress Google Maps Plugin < 8.1.12 Multiple XSS Vulnerabilities

Summary
The WordPress plugin Google Maps is prone to multiple cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.25
Fixed version:     8.1.12
Installation
path / port:       /costa/wordpress/wp-content/plugins/wp-google-maps
```

Solution:
Solution type: VendorFix
Update to version 8.1.12 or later.

Affected Software/OS
WordPress Google Maps plugin version 8.1.11 and prior.

Vulnerability Detection Method
Details: `WordPress Google Maps Plugin < 8.1.12 Multiple XSS Vulnerabilities`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.146811
Version used: 2021-09-30T13:01:29Z

References

```
cve: CVE-2021-24383
cve: CVE-2021-36871
url: https://wpscan.com/vulnerability/1270588c-53fe-447e-b83c-1b877dc7a954
url: https://patchstack.com/database/vulnerability/wp-google-maps-pro/wordpress-
↪wp-google-maps-pro-premium-plugin-8-1-11-multiple-authenticated-persistent-cro
↪ss-site-scripting-xss-vulnerabilities
url: https://wordpress.org/plugins/wp-google-maps/#developers
```

Medium (CVSS: 5.3)
NVT: MacOS X Finder '.DS_Store' Information Disclosure

Summary

MacOS X creates a hidden file '.DS_Store', in each directory that has been viewed with the 'Finder'. This file contains a list of the contents of the directory, giving an attacker information on the structure and contents of your website.

Vulnerability Detection Result

```
The following files were identified:
https://staff.icar.cnr.it/tmp/upload/.DS_Store
https://staff.icar.cnr.it/tmp/uploadmsc/.DS_Store
```

Solution:

Solution type: Workaround

Block access to hidden files (starting with a dot) within your webservers configuration

Vulnerability Detection Method

Details: `MacOS X Finder '.DS_Store' Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.10756
Version used: 2021-07-05T11:01:33Z

References

```
cve: CVE-2016-1776
cve: CVE-2018-6470
bid: 3316
bid: 3324
bid: 85054
url: https://www.securityfocus.com/bid/3316
url: https://www.securityfocus.com/bid/3324
url: https://www.securityfocus.com/bid/85054
url: https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html
url: https://support.apple.com/en-us/HT1629
cert-bund: CB-K16/0450
```

. . . continues on next page . . .

. . . continued from previous page . . .

dfn-cert: DFN-CERT-2016-0489

Medium (CVSS: 5.0)
NVT: Backup File Scanner (HTTP) - Reliable Detection Reporting

Summary
The script reports backup files left on the web server.
Notes:
- 'Reliable Detection' means that a file was detected based on a strict (regex) and reliable pattern matching the response of the remote web server when a file was requested.
- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Result

```
The following backup files were identified (<URL>:<Matching pattern>):
https://staff.icar.cnr.it/folino/apsb/base.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/apsb/config.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/apsb/esame.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/apsb/forum/forum.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/apsb/index.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/apsb/lezioni.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/apsb/materialeupload.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/apsb/news.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/config.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/lso/base.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/lso/config.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/lso/esame.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/lso/index.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/lso/lezioni.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/lso/materialeupload.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/lso/news.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/msc/base.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/msc/config.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/msc/esame.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/msc/index.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/msc/lezioni.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/msc/materialeupload.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/msc/news.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/selab/config.php.bak:^<\?(php|=)
https://staff.icar.cnr.it/folino/selab/config.php.save:^<\?(php|=)
https://staff.icar.cnr.it/folino/selab/index.php.bak:^<\?(php|=)
```

Impact
Based on the information provided in this files an attacker might be able to gather sensitive information stored in these files.

Solution:

. . . continues on next page . . .

. . . continued from previous page . . .

Solution type: Mitigation
Delete the backup files.

Vulnerability Detection Method
Reports previous enumerated backup files accessible on the remote web server.
Details: `Backup File Scanner (HTTP) - Reliable Detection Reporting`
OID:1.3.6.1.4.1.25623.1.0.108976
Version used: `2021-01-21T10:06:42Z`

References
`url: http://www.openwall.com/lists/oss-security/2017/10/31/1`

Medium (CVSS: 5.0)
NVT: Linux Home Folder Accessible

Summary
The script attempts to identify files of a linux home folder accessible at the webserver.

Vulnerability Detection Result

```
The following files were identified:
https://staff.icar.cnr.it/staff/ant/.ssh/authorized_keys
https://staff.icar.cnr.it/staff/mastroianni/.ssh/authorized_keys
https://staff.icar.cnr.it/staff/sacca/.ssh/authorized_keys
```

Impact
Based on the information provided in this files an attacker might be able to gather additional info.

Solution:
Solution type: Mitigation
A users home folder shouldn't be accessible via a webserver. Restrict access to it or remove it completely.

Vulnerability Insight
Currently the script is checking for the following files:
- /.ssh/authorized_keys
- /.ssh/config
- /.ssh/known_hosts
- /.ssh/identity
- /.ssh/id_rsa
- /.ssh/id_rsa.pub
- /.ssh/id_dsa
- /.ssh/id_dsa.pub
- /.ssh/id_dss
- /.ssh/id_dss.pub

. . . continues on next page . . .

. . . continued from previous page . . .

- /.ssh/id_ecdsa
- /.ssh/id_ecdsa.pub
- /.ssh/id_ed25519
- /.ssh/id_ed25519.pub
- /.mysql_history
- /.sqlite_history
- /.psql_history
- /.sh_history
- /.bash_history
- /.profile
- /.bashrc

Vulnerability Detection Method

Check the response if files from a home folder are accessible.

Details: `Linux Home Folder Accessible`

OID:1.3.6.1.4.1.25623.1.0.111108

Version used: `2021-02-02T12:11:39Z`

Medium (CVSS: 4.8)

NVT: WordPress Download Manager Plugin < 3.2.16 XSS Vulnerability

Summary

The WordPress plugin Download Manager is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 3.1.03
Fixed version:     3.2.16
Installation
path / port:       /costa/wordpress/wp-content/plugins/download-manager
```

Impact

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

Solution:

Solution type: VendorFix

Update to version 3.2.16 or later.

Affected Software/OS

WordPress Download Manager plugin prior to version 3.2.16.

Vulnerability Insight

The plugin does not escape some of the Download settings when outputting them, allowing high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

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

Details: `WordPress Download Manager Plugin < 3.2.16 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.147157

Version used: `2021-11-15T10:21:31Z`

References

```
cve: CVE-2021-24773
url: https://wpscan.com/vulnerability/aab2ddbb-7675-40fc-90ee-f5bfa8a5b995
url: https://wordpress.org/plugins/download-manager/#developers
```

Medium (CVSS: 4.8)

NVT: WordPress Duplicate Page Plugin < 4.4.3 XSS Vulnerability

Summary

The WordPress plugin Duplicate Page is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2
Fixed version:     4.4.3
Installation
path / port:       /costa/wordpress/wp-content/plugins/duplicate-page
```

Solution:

Solution type: VendorFix

Update to version 4.4.3 or later.

Affected Software/OS

WordPress Duplicate Page version 4.4.2 and prior.

Vulnerability Insight

The plugin does not sanitise or escape the Duplicate Post Suffix settings before outputting it, which could allow high privilege users to perform stored cross-site scripting attacks even when the unfiltered_html capability is disallowed.

Vulnerability Detection Method

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

Details: `WordPress Duplicate Page Plugin < 4.4.3 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.147031

Version used: `2021-10-29T14:03:48Z`

References

```
cve: CVE-2021-24681
url: https://wpscan.com/vulnerability/9ebdd1df-1d6f-4399-8b0f-77a79f841464
url: https://wordpress.org/plugins/duplicate-page/#developers
```

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`

References

```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
```

. . . continues on next page . . .

. . . continued from previous page . . .

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:                 1.2.840.113549.1.9.1=#67656E74696C6540696361722E636E722E69
↪74,CN=staff.icar.cnr.it,OU=icarCNR,O=icarCNR,L=Cosenza,ST=Italy,C=IT
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1, Fingerprint2

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-10-15T11:13:32Z`

References

```
url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-
↪sha-1-based-signature-algorithms/
```

[return to 150.145.63.3]

2.1.4 Medium 80/tcp

Medium (CVSS: 6.8)
NVT: WordPress TablePress Plugin < 1.10 CSV Injection Vulnerability

Summary

The WordPress plugin TablePress is prone to a CSV injection vulnerability.

Vulnerability Detection Result

```
Installed version: 1.9.2
Fixed version:     1.10
Installation
path / port:       /costa/wordpress/wp-content/plugins/tablepress
```

Impact

Successful exploitation would allow an attacker to force an unknown user to execute code on the affected device.

Solution:
Solution type: VendorFix
Update to version 1.10 or later.

Affected Software/OS

WordPress TablePress plugin before version 1.10.

Vulnerability Detection Method

Details: `WordPress TablePress Plugin < 1.10 CSV Injection Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.112685
Version used: `2021-07-07T02:00:46Z`

References

```
cve: CVE-2019-20180
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://wordpress.org/plugins/tablepress/#developers
url: https://medium.com/@Pablo0xSantiago/cve-2019-20180-tablepress-version-1-9-2
↪-csv-injection-65309fcc8be8
```

Medium (CVSS: 6.1)
NVT: WordPress All In One WP Security & Firewall Plugin < 4.4.6 XSS Vulnerability

Summary
The WordPress plugin All In One WP Security & Firewall is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 4.4.4
Fixed version:     4.4.6
Installation
path / port:       /costa/wordpress/wp-content/plugins/all-in-one-wp-security-an
↪d-firewall
```

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

Solution:
Solution type: VendorFix
Update to version 4.4.6.

Affected Software/OS
WordPress All In One WP Security & Firewall plugin through 4.4.5.

Vulnerability Insight
The vulnerability is exploitable via the wp-security-blacklist-menu.php page.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress All In One WP Security & Firewall Plugin < 4.4.6 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.113788
Version used: `2021-08-17T12:00:57Z`

References

```
cve: CVE-2020-29171
url: https://github.com/Arsenal21/all-in-one-wordpress-security/commit/4130906bc
↪049b195467b4fc6980d6d304fbe28d5
url: https://wordpress.org/plugins/all-in-one-wp-security-and-firewall
```

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
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: `2021-02-15T07:14:40Z`

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
bid: 9506
bid: 9561
bid: 11604
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
bid: 15222
bid: 19915
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
url: http://www.kb.cert.org/vuls/id/288308
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: 5.8)
NVT: WordPress User IDs and User Names Disclosure

Summary
WordPress platforms use a parameter called 'author'. This parameter accepts integer values and represents the 'User ID' of users in the web site. For example: http://www.example.com/?author=1

Vulnerability Detection Result

```
The following user names were revealed in id range 1-25.
Discovered username 'gc_user_1' with id '1'
```

Impact
These problems trigger the following attack vectors:
1. The query response discloses whether the User ID is enabled.
2. The query response leaks (by redirection) the User Name corresponding with that User ID.

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

Vulnerability Insight
The problems found are:
1. User ID values are generated consecutively.

. . . continues on next page . . .

. . . continued from previous page . . .

2. When a valid User ID is found, WordPress redirects to a web page with the name of the author.

Vulnerability Detection Method

Details: `WordPress User IDs and User Names Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103222

References

```
url: http://www.talsoft.com.ar/index.php/research/security-advisories/wordpress-
↪user-id-and-user-name-disclosure
```

Medium (CVSS: 5.4)
NVT: WordPress Google Maps Plugin < 8.1.12 Multiple XSS Vulnerabilities

Summary

The WordPress plugin Google Maps is prone to multiple cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.25
Fixed version:     8.1.12
Installation
path / port:       /costa/wordpress/wp-content/plugins/wp-google-maps
```

Solution:
Solution type: VendorFix
Update to version 8.1.12 or later.

Affected Software/OS

WordPress Google Maps plugin version 8.1.11 and prior.

Vulnerability Detection Method

Details: `WordPress Google Maps Plugin < 8.1.12 Multiple XSS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.146811
Version used: `2021-09-30T13:01:29Z`

References

```
cve: CVE-2021-24383
cve: CVE-2021-36871
url: https://wpscan.com/vulnerability/1270588c-53fe-447e-b83c-1b877dc7a954
url: https://patchstack.com/database/vulnerability/wp-google-maps-pro/wordpress-
↪wp-google-maps-pro-premium-plugin-8-1-11-multiple-authenticated-persistent-cro
↪ss-site-scripting-xss-vulnerabilities
url: https://wordpress.org/plugins/wp-google-maps/#developers
```

Medium (CVSS: 5.4)
NVT: WordPress Google Maps Plugin < 8.1.13 XSS Vulnerability

Summary
The WordPress plugin Google Maps is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 8.0.25
Fixed version:     8.1.13
Installation
path / port:       /costa/wordpress/wp-content/plugins/wp-google-maps
```

Solution:
Solution type: VendorFix
Update to version 8.1.13 or later.

Affected Software/OS
WordPress Google Maps plugin version 8.1.12 and prior.

Vulnerability Detection Method
Details: `WordPress Google Maps Plugin < 8.1.13 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.146812
Version used: `2021-09-30T13:01:29Z`

References

```
cve: CVE-2021-36870
url: https://patchstack.com/database/vulnerability/wp-google-maps/wordpress-wp-g
↪oogle-maps-plugin-8-1-12-multiple-authenticated-persistent-cross-site-scriptin
↪g-xss-vulnerabilities
url: https://wordpress.org/plugins/wp-google-maps/#developers
```

Medium (CVSS: 5.3)
NVT: MacOS X Finder '.DS_Store' Information Disclosure

Summary
MacOS X creates a hidden file '.DS_Store', in each directory that has been viewed with the 'Finder'. This file contains a list of the contents of the directory, giving an attacker information on the structure and contents of your website.

Vulnerability Detection Result

```
The following files were identified:
http://staff.icar.cnr.it/tmp/upload/.DS_Store
http://staff.icar.cnr.it/tmp/uploadmsc/.DS_Store
```

Solution:
Solution type: Workaround

. . . continues on next page . . .

. . . continued from previous page . . .

Block access to hidden files (starting with a dot) within your webservers configuration

Vulnerability Detection Method

Details: `MacOS X Finder '.DS_Store' Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.10756
Version used: `2021-07-05T11:01:33Z`

References

```
cve: CVE-2016-1776
cve: CVE-2018-6470
bid: 3316
bid: 3324
bid: 85054
url: https://www.securityfocus.com/bid/3316
url: https://www.securityfocus.com/bid/3324
url: https://www.securityfocus.com/bid/85054
url: https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html
url: https://support.apple.com/en-us/HT1629
cert-bund: CB-K16/0450
dfn-cert: DFN-CERT-2016-0489
```

Medium (CVSS: 5.0)
NVT: Linux Home Folder Accessible

Summary

The script attempts to identify files of a linux home folder accessible at the webserver.

Vulnerability Detection Result

```
The following files were identified:
http://staff.icar.cnr.it/staff/ant/.ssh/authorized_keys
http://staff.icar.cnr.it/staff/mastroianni/.ssh/authorized_keys
http://staff.icar.cnr.it/staff/sacca/.ssh/authorized_keys
```

Impact

Based on the information provided in this files an attacker might be able to gather additional info.

Solution:

Solution type: Mitigation

A users home folder shouldn't be accessible via a webserver. Restrict access to it or remove it completely.

Vulnerability Insight

Currently the script is checking for the following files:
- /.ssh/authorized_keys

. . . continues on next page . . .

. . . continued from previous page . . .

- /.ssh/config
- /.ssh/known_hosts
- /.ssh/identity
- /.ssh/id_rsa
- /.ssh/id_rsa.pub
- /.ssh/id_dsa
- /.ssh/id_dsa.pub
- /.ssh/id_dss
- /.ssh/id_dss.pub
- /.ssh/id_ecdsa
- /.ssh/id_ecdsa.pub
- /.ssh/id_ed25519
- /.ssh/id_ed25519.pub
- /.mysql_history
- /.sqlite_history
- /.psql_history
- /.sh_history
- /.bash_history
- /.profile
- /.bashrc

Vulnerability Detection Method

Check the response if files from a home folder are accessible.
Details: `Linux Home Folder Accessible`
OID:1.3.6.1.4.1.25623.1.0.111108
Version used: `2021-02-02T12:11:39Z`

Medium (CVSS: 5.0)
NVT: Backup File Scanner (HTTP) - Reliable Detection Reporting

Summary

The script reports backup files left on the web server.
Notes:
- 'Reliable Detection' means that a file was detected based on a strict (regex) and reliable pattern matching the response of the remote web server when a file was requested.
- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Result

```
The following backup files were identified (<URL>:<Matching pattern>):
http://staff.icar.cnr.it/folino/apsb/base.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/apsb/config.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/apsb/esame.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/apsb/forum/forum.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/apsb/index.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/apsb/lezioni.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/apsb/materialeupload.php.bak:^<\?(php|=)
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://staff.icar.cnr.it/folino/apsb/news.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/config.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/lso/base.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/lso/config.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/lso/esame.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/lso/index.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/lso/lezioni.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/lso/materialeupload.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/lso/news.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/msc/base.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/msc/config.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/msc/esame.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/msc/index.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/msc/lezioni.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/msc/materialeupload.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/msc/news.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/selab/config.php.bak:^<\?(php|=)
http://staff.icar.cnr.it/folino/selab/config.php.save:^<\?(php|=)
http://staff.icar.cnr.it/folino/selab/index.php.bak:^<\?(php|=)
```

Impact

Based on the information provided in this files an attacker might be able to gather sensitive information stored in these files.

Solution:

Solution type: Mitigation

Delete the backup files.

Vulnerability Detection Method

Reports previous enumerated backup files accessible on the remote web server.

Details: `Backup File Scanner (HTTP) - Reliable Detection Reporting`

OID:1.3.6.1.4.1.25623.1.0.108976

Version used: `2021-01-21T10:06:42Z`

References

url: `http://www.openwall.com/lists/oss-security/2017/10/31/1`

Medium (CVSS: 4.8)

NVT: WordPress Download Manager Plugin < 3.2.16 XSS Vulnerability

Summary

The WordPress plugin Download Manager is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 3.1.03
Fixed version:     3.2.16
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Installation
path / port:       /costa/wordpress/wp-content/plugins/download-manager
```

Impact

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

Solution:

Solution type: VendorFix

Update to version 3.2.16 or later.

Affected Software/OS

WordPress Download Manager plugin prior to version 3.2.16.

Vulnerability Insight

The plugin does not escape some of the Download settings when outputting them, allowing high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed

Vulnerability Detection Method

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

Details: `WordPress Download Manager Plugin < 3.2.16 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.147157

Version used: `2021-11-15T10:21:31Z`

References

```
cve: CVE-2021-24773
url: https://wpscan.com/vulnerability/aab2ddbb-7675-40fc-90ee-f5bfa8a5b995
url: https://wordpress.org/plugins/download-manager/#developers
```

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

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

Vulnerability Detection Result

```
The following URLs requires Basic Authentication (URL:realm name):
http://staff.icar.cnr.it/phpmyadmin:"Restricted Files"
```

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

. . . continues on next page . . .

. . . continued from previous page . . .

Solution:

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)

- HTTP Forms (e.g. Login) with input field of type 'password'

Details: `Cleartext Transmission of Sensitive Information via HTTP`

OID:1.3.6.1.4.1.25623.1.0.108440

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

References

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

Medium (CVSS: 4.8)

NVT: WordPress Duplicate Page Plugin < 4.4.3 XSS Vulnerability

Summary

The WordPress plugin Duplicate Page is prone to a cross-site scripting (XSS) vulnerability.

Vulnerability Detection Result

```
Installed version: 4.2
Fixed version:     4.4.3
Installation
path / port:       /costa/wordpress/wp-content/plugins/duplicate-page
```

Solution:

Solution type: VendorFix

Update to version 4.4.3 or later.

Affected Software/OS

WordPress Duplicate Page version 4.4.2 and prior.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The plugin does not sanitise or escape the Duplicate Post Suffix settings before outputting it, which could allow high privilege users to perform stored cross-site scripting attacks even when the unfiltered_html capability is disallowed.

Vulnerability Detection Method

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

Details: `WordPress Duplicate Page Plugin < 4.4.3 XSS Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.147031

Version used: `2021-10-29T14:03:48Z`

References

```
cve: CVE-2021-24681
url: https://wpscan.com/vulnerability/9ebdd1df-1d6f-4399-8b0f-77a79f841464
url: https://wordpress.org/plugins/duplicate-page/#developers
```

[return to 150.145.63.3]

2.1.5 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

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

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 2042882916
Packet 2: 2042883995
```

Impact

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

Solution:

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

. . . continues on next page . . .

. . . continued from previous page . . .

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

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

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

References

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

[return to 150.145.63.3]