



CVE-2021-41270

Published on: 11/24/2021 12:00:00 AM UTC

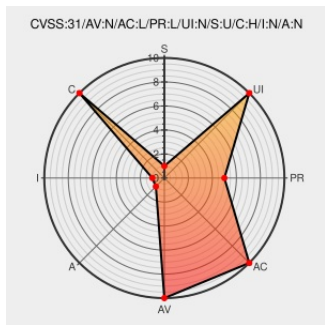
Last Modified on: 12/15/2021 05:35:00 PM UTC

CVE-2021-41270 - advisory for GHSA-2xhg-w2g5-w95x

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

Symfony/Serializer handles serializing and deserializing data structures for Symfony, a PHP framework for web and console applications and a set of reusable PHP components. Symfony versions 4.1.0 before 4.4.35 and versions 5.0.0 before 5.3.12 are vulnerable to CSV injection, also known as formula injection. In Symfony 4.1, maintainers added the opt-in `csv_escape_formulas` option in the `CsvEncoder`, to prefix all cells starting with `=`, `+`, `-` or `@` with a tab `\t`. Since then, OWASP added 2 chars in that list: Tab (0x09) and Carriage return (0x0D). This makes the previous prefix char (Tab `\t`) part of the vulnerable characters, and OWASP suggests using the single quote `'` for prefixing the value. Starting with versions 4.4.34 and 5.3.12, Symfony now follows the OWASP recommendations and uses the single quote `'` to prefix formulas and add the prefix to cells starting by `\t`, `\r` as well as `=`, `+`, `-` and `@`.

CVE-2021-41270 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **symfony** - **symfony** version $\geq 4.1.0$, $< 4.4.35$

Affected Vendor/Software: **symfony** - **symfony** version $\geq 5.0.0$, $< 5.3.12$

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

VECTOR	COMPLEXITY	
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Prevent CSV Injection via formulas · Advisory · symfony/symfony · GitHub	github.com text/html	CONFIRM github.com/symfony/symfony/security/advisories/GHSA-2xhg-w2g5-w95x
[SECURITY] Fedora 34 Update: php-symfony4-4.4.35-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-0294e8ca24
Release v5.3.12 · symfony/symfony · GitHub	github.com text/html	MISC github.com/symfony/symfony/releases/tag/v5.3.12
[SECURITY] Fedora 35 Update: php-symfony4-4.4.35-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-10fd47b32d
Release v5.3.12 by fabpot · Pull Request #44243 · symfony/symfony · GitHub	github.com text/html	MISC github.com/symfony/symfony/pull/44243
Use single quote to escape formulas · symfony/symfony@3da6f2d · GitHub	github.com text/html	MISC github.com/symfony/symfony/commit/3da6f2d45e7536ccb2a26f52fbaf340917e208a8

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[282093](#) Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2021-0294e8ca24)

[282135](#) Fedora Security Update for Hypertext Preprocessor (PHP) (FEDORA-2021-10fd47b32d)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Sensiolabs	Symfony	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:

cpe:2.3:a:sensiolabs:symfony:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @symfony	CVE-2021-41270: Prevent CSV Injection via formulas symfony.com/blog/cve-2021-... #symfony	2021-11-24 09:13:12
 @websagiles	CVE-2021-41270: Prevent CSV Injection via formulas dlvr.it/SD5tBk https://t.co/gEyzx0rRRN	2021-11-24 11:13:41
 @CVEreport	CVE-2021-41270 : Symfony/Serializer handles serializing and deserializing data structures for Symfony, a PHP framew... twitter.com/i/web/status/1...	2021-11-24 19:11:53
 /r/symfony	CVE-2021-41270: Prevent CSV Injection via formulas	2021-11-24 10:00:10

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)