

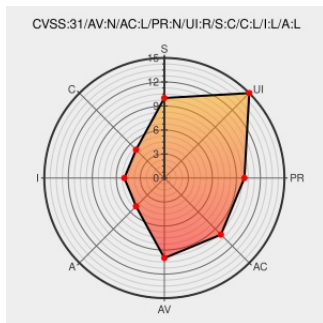


CVE-2022-3026

Published on: Not Yet Published

Last Modified on: 09/09/2022 02:32:00 AM UTC

CVE-2022-3026

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Wp-users-exporter](#) from [Wp-users-exporter Project](#) contain the following vulnerability:

The WP Users Exporter plugin for WordPress is vulnerable to CSV Injection in versions up to, and including, 1.4.2 via the 'Export Users' functionality. This makes it possible for authenticated attackers, such as a subscriber, to add untrusted input into profile information like First Names that will embed into the exported CSV file triggered by an administrator and can result in code execution when these files are downloaded and opened on a local system with a vulnerable configuration.

CVE-2022-3026 has been assigned by [security@wordfence.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [leogermani](#) - **WP Users Exporter** version $\leq 1.4.2$

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/wp-users-exporter/trunk/A_UserExporter.class.php
Vulnerability Advisories - Wordfence	www.wordfence.com text/html	MISC www.wordfence.com/vulnerability-advisories/#CVE-2022-3026

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

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or content 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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

```
cve update exploit poc rce sqli code cve-2022-3026 Log4j jndi rmi
`mysql://root:123djnes71dsaasj@mysql.tencent.com` 辣...
```

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-users-exporter Project	Wp-users-exporter	All	All	All	All
cpe:2.3:a:wp-users-exporter_project:wp-users-exporter:*:*:*:*:wordpress:*:*:						

Discovery Credit

Zhouyuan Yang

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-3026 : The WP Users Exporter plugin for WordPress is vulnerable to CSV Injection in versions up to, and in... twitter.com/i/web/status/1...	2022-09-06 18:16:25
 @LinInfoSec	Wordpress - CVE-2022-3026: wordfence.com/vulnerability-...	2022-09-06 21:00:59

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)