



CVE-2020-22277

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-22277
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-04 17:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	Import and export users and customers WordPress Plugin through 1.15.5.11 allows CSV injection via a customer's profile.

Risk And Classification

Problem Types: CWE-1236

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codecton	Import And Export Users And Customers	All	All	All	All

References

Reference	Source	Link	Tags
WordPress › Import users from CSV with meta ‹ WordPress Plugins	MISC	wordpress.org	Product, Release Notes, Third P
cert.ikiu.ac.ir/public-files/news/document/CVE-99/CVE-2020-22277.pdf	MISC	cert.ikiu.ac.ir	Exploit, Third Party Advisory
mega.nz/file/bSQnIS4R	MISC	mega.nz	Exploit, Third Party Advisory
Import and export users and customers – WordPress plugin WordPress.org		wordpress.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

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