CVE-2022-25241

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-25241
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-16 02:15:00 UTC
Updated	2022-02-23 21:00:00 UTC
Description	In FileCloud before 21.3, the CSV user import functionality is vulnerable to Cross-Site Request Forgery (CSRF).

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Filecloud	Filecloud	All	All	All	All

References

Reference	Source	Link	Tags
FileCloud 21.2 Cross Site Request Forgery ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party Adviso
Advisory 2022-01-3 Threat of CSRF via User Creation - FileCloud Docs	MISC	www.filecloud.com	Vendor Advisory
herolab.usd.de/security-advisories	MISC	herolab.usd.de	Third Party Advisory
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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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