



CVE-2021-3150

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

Summary

CVE	CVE-2021-3150
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-15 19:15:00 UTC
Updated	2021-12-03 17:58:00 UTC
Description	A cross-site scripting (XSS) vulnerability on the Delete Personal Data page in Cryptshare Server before 4.8.0 allows an atta

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cryptshare	Cryptshare Server	All	All	All	All

References

Reference	Source	Link
Update from v4.7.1 to v4.8.1 - Cryptshare Server Manual - Cryptshare Documentation	MISC	wiki.cryptshare.cc
McAfee Security Bulletin - Status and updates for OpenSSL vulnerabilities (CVE-2021-3450 and 2021-3449)	CONFIRM	kc.mcafee.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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