



CVE-2020-35950

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

Summary

CVE	CVE-2020-35950
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-01 04:15:00 UTC
Updated	2021-01-13 16:51:00 UTC
Description	An issue was discovered in the XCloner Backup and Restore plugin before 4.2.153 for WordPress. It allows CSRF (via almu

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
XCloner Backup and Restore < 4.2.153 - Cross-Site Request Forgery Security Vulnerability	MISC	wpscan.com	Exploit, Thi
Critical Vulnerabilities Patched in XCloner Backup and Restore Plugin	MISC	www.wordfence.com	Exploit, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, i

No vendor comments have been submitted for this CVE.

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

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