



CVE-2020-8789

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

Summary

CVE	CVE-2020-8789
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-22 14:15:00 UTC
Updated	2021-04-08 16:36:00 UTC
Description	Composr 10.0.30 allows Persistent XSS via a Usergroup name under the Security configuration.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Composr Project	Composr	All	All	All	All
Application	Ocproducts	Composr	All	All	All	All

References

Reference	Source	Link	Tags
Full Disclosure: Composr CMS 10.0.30 - (Authenticated) Cross-Site Scripting	FULLDISC	seclists.org	Exploit, Mailing List,
Composr CMS 10.0.30 Cross Site Scripting ~ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party /
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 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