CVE-2020-12816

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-12816
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-24 15:15:00 UTC
Updated	2020-09-30 22:51:00 UTC
Description	An improper neutralization of input vulnerability in FortiNAC before 8.7.2 may allow a remote authenticated attacker to perfo

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortinac	All	All	All	All
Application	Fortinet	Fortinac	All	All	All	All

References

Reference	Source	Link	Tags
XSS vulnerability in the UserID of Admin Users in FortiNAC | FortiGuard	CONFIRM	fortiguard.com	Vendor Advisory
XSS vulnerability in the UserID of Admin Users in FortiNAC | FortiGuard	MISC	www.fortiguard.com	Vendor 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.

CVE.report and Source URL Uptime Status status.cve.report