CVE-2021-22128

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-22128
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-04 18:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	An improper access control vulnerability in FortiProxy SSL VPN portal 2.0.0, 1.2.9 and below versions may allow an authen

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortiproxy	2.0.0	All	All	All
Application	Fortinet	Fortiproxy	2.0.0	All	All	All
Application	Fortinet	Fortiproxy	All	All	All	All

References

Reference	Source	Link
FortiProxy SSL-VPN Improper Access Control vulnerability through the Quick connection functionality | FortiGuard	CONFIRM	fortiguard.c
CVE Program record	CVE.ORG	www.cve.or
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.report and Source URL Uptime Status status.cve.report