



CVE-2021-36177

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

Summary

CVE	CVE-2021-36177
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-02 11:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	An improper access control vulnerability [CWE-284] in FortiAuthenticator HA service 6.3.2 and below, 6.2.x, 6.1.x, 6.0.x ma

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
PSIRT Advisories FortiGuard	CONFIRM	fortiguard.com	
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.

Legacy QID Mappings

[379375](#) FortiAuthenticator Improper access control in HA service (FG-IR-20-217)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)