



CVE-2021-24012

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

Summary

CVE	CVE-2021-24012
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-02 13:15:00 UTC
Updated	2021-06-14 14:56:00 UTC
Description	An improper following of a certificate's chain of trust vulnerability in FortiGate versions 6.4.0 to 6.4.4 may allow an LDAP us

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All

References

Reference	Source	Lin
FortiOS - Improper verification of the user certificate's chain of trust in FortiGate when connecting to SSL-VPN FortiGuard	CONFIRM	fort
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

44096 FortiOS - Improper Verification Of Chain Of Trust of User Certificate Vulnerability (FG-IR-21-018)

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](#)