



CVE-2021-41024

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

Summary

CVE	CVE-2021-41024
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-08 13:15:00 UTC
Updated	2021-12-09 19:26:00 UTC
Description	A relative path traversal [CWE-23] vulnerability in FortiOS versions 7.0.0 and 7.0.1 and FortiProxy version 7.0.0 may allow a

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	7.0.0	All	All	All
Operating System	Fortinet	Fortios	7.0.1	All	All	All
Application	Fortinet	Fortiproxy	7.0.0	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

[43909](#) FortiOS Path Traversal Vulnerability (FG-IR-21-181)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

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