

CVE-2022-41328

Fortinet FortiOS Path Traversal Vulnerability

CISA KEV since Mar 14, 2023

Actively exploited

A improper limitation of a pathname to a restricted directory vulnerability ('path traversal') [CWE-22] in Fortinet FortiOS version 7.2.0 through 7.2.3, 7.0.0 through 7.0.9 and before 6.4.11 allows a privileged attacker to read and write files on the underlying Linux system via crafted CLI commands.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.1 High · NVD	EPSS 0.107 95.8th percentile · FIRST	CISA DEADLINE Apr 4, 2023 KEV since 2023 · listed over a year
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.107 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortios	$\geq 6.0.0 \leq 6.0.16$ $\geq 6.2.0 < 6.2.14$ $\geq 6.4.0 < 6.4.12$ $\geq 7.0.0 < 7.0.10$ $\geq 7.2.0 < 7.2.4$	after 6.0.16 · 6.2.14 · 6.4.12 · 7.0.10 · 7.2.4	NVD

Sources

Vendor guidance github.com/advisories/GHSA-prj2-6g47-x68h
fortiguard.com fortiguard.com/psirt/FG-IR-22-369
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2022-41328

Additional guidance fortiguard.com/psirt/FG-IR-22-369
NVD nvd.nist.gov/vuln/detail/CVE-2022-41328
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-44535

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.