

CVE-2024-21762

Fortinet FortiOS Out-of-Bound Write Vulnerability

Exigent

CISA KEV since Feb 9, 2024

Actively exploited

Ransomware use known

A out-of-bounds write vulnerability in Fortinet FortiOS 7.4.0 through 7.4.2, FortiOS 7.2.0 through 7.2.6, FortiOS 7.0.0 through 7.0.13, FortiOS 6.4.0 through 6.4.14, FortiOS 6.2.0 through 6.2.15, FortiOS 6.0 all versions, FortiProxy 7.4.0 through 7.4.2, FortiProxy 7.2.0 through 7.2.8, FortiProxy 7.0.0 through 7.0.14, FortiProxy 2.0.0 through 2.0.13, FortiProxy 01.02 all versions, FortiProxy 1.2 all versions, FortiProxy 01.01 all versions, FortiProxy 1.1 all versions, FortiProxy 01.00 all versions allows attacker to execute unauthorized code or commands via specifically crafted requests

EVRS 89/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.834 99.68th percentile · FIRST	CISA DEADLINE Feb 16, 2024 KEV since 2024 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.834 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortiproxy	≥ 1.0.0 < 2.0.14 ≥ 7.0.0 < 7.0.15 ≥ 7.2.0 < 7.2.9 ≥ 7.4.0 < 7.4.3	2.0.14 · 7.0.15 · 7.2.9 · 7.4.3	NVD
fortios	≥ 6.0.0 < 6.0.18 ≥ 6.2.0 < 6.2.16 ≥ 6.4.0 < 6.4.15 ≥ 7.0.0 < 7.0.14 ≥ 7.2.0 < 7.2.7 ≥ 7.4.0 < 7.4.3	6.0.18 · 6.2.16	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-v4hq-m4wr-6pmj	Additional guidance	fortiguard.com/psirt/FG-IR-24-015
fortiguard.fortinet.com	fortiguard.fortinet.com/psirt/FG-IR-24-015	NVD	nvd.nist.gov/vuln/detail/CVE-2024-21762
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-19376
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-21762		

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