

CVE-2022-42475

Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability

Exigent

CISA KEV since Dec 13, 2022

Actively exploited

Ransomware use known

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS SSL-VPN 7.2.0 through 7.2.2, 7.0.0 through 7.0.8, 6.4.0 through 6.4.10, 6.2.0 through 6.2.11, 6.0.15 and earlier and FortiProxy SSL-VPN 7.2.0 through 7.2.1, 7.0.7 and earlier may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests.

EVRS 94/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.995 99.94th percentile · FIRST	CISA DEADLINE Jan 3, 2023 KEV since 2022 · 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	0.995 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 15 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortiproxy	$\geq 1.0.0 \leq 1.0.7$ $\geq 1.1.0 \leq 1.1.6$ $\geq 1.2.0 \leq 1.2.13$ $\geq 2.0.0 < 2.0.12$ $\geq 7.0.0 < 7.0.8$ $\geq 7.2.0 < 7.2.2$	no fixed version listed	NVD
fortios	$\geq 5.0.0 \leq 5.0.14$ $\geq 5.2.0 \leq 5.2.15$ $\geq 5.4.0 \leq 5.4.13$ $\geq 5.6.0 \leq 5.6.14$ $\geq 6.0.0 < 6.0.16$ $\geq 6.2.0 < 6.2.12$ $\geq 6.4.0 < 6.4.11$ $\geq 7.0.0 < 7.0.9$ $\geq 7.2.0 < 7.2.3$ $\geq 6.0.0 < 6.0.15$ $\geq 6.4.0 < 6.4.10$ $\geq 7.0.0 < 7.0.8$	after 5.0.14 · after 5.2.15 · after 5.4.13 · after 5.6.14 · 6.0.16 · 6.2.12	NVD
fim-7901e	—	no fixed version listed	NVD
fim-7904e	—	no fixed version listed	NVD
fim-7910e	—	no fixed version listed	NVD
fim-7920e	—	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
fim-7921f	–	no fixed version listed	NVD
fim-7941f	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-p3vq-4cxh-gfp9	Additional guidance	fortiguard.com/psirt/FG-IR-22-398
fortiguard.com	fortiguard.com/psirt/FG-IR-22-398	NVD	nvd.nist.gov/vuln/detail/CVE-2022-42475
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-45545
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-42475		

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