

CVE-2023-27997

Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability

Exigent

CISA KEV since Jun 13, 2023

Actively exploited

Ransomware use known

A heap-based buffer overflow vulnerability [CWE-122] in FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.

EVRs

90/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.857

99.73rd percentile · FIRST

CISA DEADLINE

Jul 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.857 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortiproxy	≥ 1.1.0 ≤ 1.1.6 ≥ 1.2.0 ≤ 1.2.13 ≥ 2.0.0 ≤ 2.0.12 ≥ 7.0.0 ≤ 7.0.9 ≥ 7.2.0 ≤ 7.2.3	after 1.1.6 · after 1.2.13 · after 2.0.12 · after 7.0.9 · after 7.2.3	NVD
fortios	≥ 6.0.0 ≤ 6.0.16 ≥ 6.2.0 ≤ 6.2.13 ≥ 6.4.0 ≤ 6.4.12 ≥ 7.0.0 ≤ 7.0.11 ≥ 7.2.0 ≤ 7.2.4 ≥ 6.0.12 ≤ 6.0.16 ≥ 6.2.9 ≤ 6.2.13 6.0.10 6.2.4 6.2.6 6.2.7 6.4.2 6.4.6 6.4.8 6.4.10 6.4.12 7.0.5 7.0.10	after 6.0.16	NVD



PACKAGE	AFFECTED	FIXED IN	SOURCE
fortigate 6000	–	no fixed version listed	NVD
fortigate 7000	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-2hj2-fcr9-9p35	Additional guidance	fortiguard.com/psirt/FG-IR-23-097
fortiguard.com	fortiguard.com/psirt/FG-IR-23-097	NVD	nvd.nist.gov/vuln/detail/CVE-2023-27997
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-31722
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-27997		

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