

CVE-2024-23113

Fortinet Multiple Products Format String Vulnerability

CISA KEV since Oct 9, 2024

Actively exploited

A use of externally-controlled format string in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, FortiPAM versions 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiSwitchManager versions 7.2.0 through 7.2.3, 7.0.0 through 7.0.3 allows attacker to execute unauthorized code or commands via specially crafted packets.

EVRS 77/100 Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.617 99.17th percentile · FIRST	CISA DEADLINE Oct 30, 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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.617 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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	$\geq 7.0.0 \leq 7.0.14$ $\geq 7.2.0 \leq 7.2.8$ $\geq 7.4.0 \leq 7.4.2$	after 7.0.14 · after 7.2.8 · after 7.4.2	NVD
fortiswitchmanager	$\geq 7.0.0 \leq 7.0.3$ $\geq 7.2.0 \leq 7.2.3$	after 7.0.3 · after 7.2.3	NVD
fortios	$\geq 7.0.0 \leq 7.0.13$ $\geq 7.2.0 \leq 7.2.6$ $\geq 7.4.0 \leq 7.4.2$	after 7.0.13	NVD
fortipam	$\geq 1.0.0 \leq 1.0.3$ $\geq 1.1.0 \leq 1.1.2$ 1.2.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-57pf-f69p-p222
fortiguard.com fortiguard.com/psirt/FG-IR-24-029
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2024-23113

Additional guidance fortiguard.com/psirt/FG-IR-24-029
NVD nvd.nist.gov/vuln/detail/CVE-2024-23113
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-20638

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