

CVE-2024-47575

Fortinet FortiManager Missing Authentication Vulnerability

Exigent CISA KEV since Oct 23, 2024 Actively exploited Public exploit module (Metasploit)

A missing authentication for critical function in FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, Fortinet FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.12, FortiManager Cloud 6.4.1 through 6.4.7 allows attacker to execute arbitrary code or commands via specially crafted requests.

EVRS 87/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.948 99.86th percentile · FIRST	CISA DEADLINE Nov 13, 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	Added to CISA KEV within the last two years
☒ EPSS	0.948 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
fortimanager	$\geq 6.2.0 < 6.2.13$ $\geq 6.4.0 < 6.4.15$ $\geq 7.0.0 < 7.0.13$ $\geq 7.2.0 < 7.2.8$ $\geq 7.4.0 < 7.4.5$ 7.6.0	6.2.13 · 6.4.15 · 7.0.13 · 7.2.8 · 7.4.5	NVD
fortimanager cloud	$\geq 6.4.1 \leq 6.4.7$ $\geq 7.0.1 < 7.0.13$ $\geq 7.2.1 < 7.2.8$ $\geq 7.4.1 < 7.4.5$	after 6.4.7	NVD

Sources

Vendor guidance github.com/advisories/GHSA-hx4q-76p6-78cc
NVD nvd.nist.gov/vuln/detail/CVE-2024-47575

Additional guidance fortiguard.fortinet.com/psirt/FG-IR-24-423
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-42531

Current data evulnable.com/vulnerability-management/cve/CVE-2024-47575

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