

CVE-2023-48788

Fortinet FortiClient EMS SQL Injection Vulnerability

Exigent
CISA KEV since Mar 25, 2024
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.

EVRS 93 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.984 99.92nd percentile · FIRST	CISA DEADLINE Apr 15, 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	0.984 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
forticlient enterprise	≥ 7.0.1 < 7.0.11	7.0.11 · 7.2.3	NVD
management server	≥ 7.2.0 < 7.2.3		

Sources

Vendor guidance	github.com/advisories/GHSA-fv47-jg3j-5qf6	Additional guidance	fortiguard.com/psirt/FG-IR-24-007
fortiguard.com	fortiguard.com/psirt/FG-IR-24-007	NVD	nvd.nist.gov/vuln/detail/CVE-2023-48788
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-52821
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-48788		

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