

CVE-2026-21643

Fortinet FortiClient EMS SQL Injection Vulnerability

Exigent

CISA KEV since Apr 13, 2026

Actively exploited

An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiClientEMS 7.4.4 may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.

EVRS 88/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.939 99.85th percentile · FIRST	CISA DEADLINE Apr 16, 2026 CISA federal deadline · Overdue by 6 months
--	--	---	--

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 year
☒ EPSS	0.939 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, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
forticlientems	7.4.4	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-r6vr-hwpr-qqch
NVD nvd.nist.gov/vuln/detail/CVE-2026-21643

Additional guidance fortiguard.fortinet.com/psirt/FG-IR-25-1142
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-5681

Current data evulnable.com/vulnerability-management/cve/CVE-2026-21643

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