

CVE-2025-25257

Fortinet FortiWeb SQL Injection Vulnerability

Exigent

CISA KEV since Jul 18, 2025

Actively exploited

An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability [CWE-89] vulnerability in Fortinet FortiWeb 7.6.0 through 7.6.3, FortiWeb 7.4.0 through 7.4.7, FortiWeb 7.2.0 through 7.2.10, FortiWeb 7.0.0 through 7.0.10 allows an unauthenticated attacker to execute unauthorized SQL code or commands via crafted HTTP or HTTPS requests.

EVRS 88/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Aug 8, 2025 KEV since 2025 · 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	0.999 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
fortiweb	≥ 7.0.0 < 7.0.11 ≥ 7.2.0 < 7.2.11 ≥ 7.4.0 < 7.4.8 ≥ 7.6.0 < 7.6.4	7.0.11 · 7.2.11 · 7.4.8 · 7.6.4	NVD

Sources

Vendor guidance github.com/advisories/GHSA-mj4r-rpwm-gg33
NVD nvd.nist.gov/vuln/detail/CVE-2025-25257

Additional guidance fortiguard.fortinet.com/psirt/FG-IR-25-151
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-21785

Current data evulnable.com/vulnerability-management/cve/CVE-2025-25257

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