

CVE-2025-58034

Fortinet FortiWeb OS Command Injection Vulnerability

CISA KEV since Nov 18, 2025

Actively exploited

Public exploit module (Metasploit)

An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.1, FortiWeb 7.6.0 through 7.6.5, FortiWeb 7.4.0 through 7.4.10, FortiWeb 7.2.0 through 7.2.11, FortiWeb 7.0.0 through 7.0.11 may allow an authenticated attacker to execute unauthorized code on the underlying system via crafted HTTP requests or CLI commands.

EVRS 75/100 Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.547 99.02nd percentile · FIRST	CISA DEADLINE Nov 25, 2025 CISA federal deadline · Overdue by 11 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	0.547 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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 < 7.0.12 ≥ 7.2.0 < 7.2.12 ≥ 7.4.0 < 7.4.11 ≥ 7.6.0 < 7.6.6 ≥ 8.0.0 < 8.0.2	7.0.12 · 7.2.12 · 7.4.11 · 7.6.6 · 8.0.2	NVD

Sources

Vendor guidance github.com/advisories/GHSA-47cr-8w72-ggmc
NVD nvd.nist.gov/vuln/detail/CVE-2025-58034

Additional guidance fortiguard.fortinet.com/psirt/FG-IR-25-513
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-198020

Current data evulnable.com/vulnerability-management/cve/CVE-2025-58034

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