

CVE-2025-59718

Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability

CISA KEV since Dec 16, 2025

Actively exploited

A improper verification of cryptographic signature vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiProxy 7.6.0 through 7.6.3, FortiProxy 7.4.0 through 7.4.10, FortiProxy 7.2.0 through 7.2.14, FortiProxy 7.0.0 through 7.0.21, FortiSwitchManager 7.2.0 through 7.2.6, FortiSwitchManager 7.0.0 through 7.0.5 allows an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML response message.

EVRS

81/100

Urgent priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.683

99.33rd percentile · FIRST

CISA DEADLINE

Dec 23, 2025

CISA federal deadline · Overdue by 10 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	0.683 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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
fortiproxy	≥ 7.0.0 < 7.0.22 ≥ 7.2.0 < 7.2.15 ≥ 7.4.0 < 7.4.11 ≥ 7.6.0 < 7.6.4	7.0.22 · 7.2.15 · 7.4.11 · 7.6.4	NVD
fortiswitchmanager	≥ 7.0.0 < 7.0.6 ≥ 7.2.0 < 7.2.7	7.0.6 · 7.2.7	NVD
fortios	≥ 7.0.0 < 7.0.18 ≥ 7.2.0 < 7.2.12 ≥ 7.4.0 < 7.4.9 ≥ 7.6.0 < 7.6.4	no fixed version listed	NVD
ruggedcom ape1808 firmware	—	no fixed version listed	NVD
ruggedcom ape1808	—	no fixed version listed	NVD



Sources

Vendor guidance github.com/advisories/GHSA-fjj2-p33c-f8qq
docs.fortinet.com docs.fortinet.com/upgrade-tool/fortigate
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2025-59718

Additional guidance fortiguard.fortinet.com/psirt/FG-IR-25-647
NVD nvd.nist.gov/vuln/detail/CVE-2025-59718
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-202198

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