

CVE-2026-24858

Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability

CISA KEV since Jan 27, 2026

Actively exploited

An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.5, FortiAnalyzer 7.4.0 through 7.4.9, FortiAnalyzer 7.2.0 through 7.2.11, FortiAnalyzer 7.0.0 through 7.0.15, FortiManager 7.6.0 through 7.6.5, FortiManager 7.4.0 through 7.4.9, FortiManager 7.2.0 through 7.2.11, FortiManager 7.0.0 through 7.0.15, FortiNAC-F 7.6.3 through 7.6.5, FortiOS 7.6.0 through 7.6.5, FortiOS 7.4.0 through 7.4.10, FortiOS 7.2.0 through 7.2.12, FortiOS

EVRS 86 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.858 99.73rd percentile · FIRST	CISA DEADLINE Jan 30, 2026 CISA federal deadline · Overdue by 9 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	0.858 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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. **CISA note:** Please adhere to Fortinet's guidelines to assess exposure and mitigate risks. Check for signs of potential compromise on all internet accessible Fortinet products affected by this vulnerability. Apply any final mitigations provided by the vendor as soon as they become available.

Basis: CISA KEV required action

7.0.0 through 7.0.18, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4.0 through 7.4.12, FortiProxy 7.2.0 through 7.2.15, FortiProxy 7.0.0 through 7.0.22, FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.0 through 7.4.11 may allow an attacker with a FortiCloud account and a registered device to log into other devices registered to other accounts, if FortiCloud SSO authentication is enabled on those devices.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortianalyzer	$\geq 7.0.0 \leq 7.0.15$ $\geq 7.2.0 \leq 7.2.11$ $\geq 7.4.0 < 7.4.10$ $\geq 7.6.0 < 7.6.6$	after 7.0.15 · after 7.2.11 · 7.4.10 · 7.6.6	NVD
fortimanager	$\geq 7.0.0 \leq 7.0.15$ $\geq 7.2.0 \leq 7.2.11$ $\geq 7.4.0 < 7.4.10$ $\geq 7.6.0 < 7.6.6$	after 7.0.15 · after 7.2.11	NVD
fortinac-f	$\geq 7.6.3 < 7.6.6$	no fixed version listed	NVD



PACKAGE	AFFECTED	FIXED IN	SOURCE
fortiproxy	$\geq 7.0.0 \leq 7.0.22$ $\geq 7.2.0 \leq 7.2.15$ $\geq 7.4.0 \leq 7.4.12$ $\geq 7.6.0 \leq 7.6.4$	no fixed version listed	NVD
fortiweb	$\geq 7.4.0 \leq 7.4.11$ $\geq 7.6.0 \leq 7.6.6$ $\geq 8.0.0 \leq 8.0.3$	no fixed version listed	NVD
fortios	$\geq 7.0.0 \leq 7.0.18$ $\geq 7.2.0 \leq 7.2.12$ $\geq 7.4.0 < 7.4.11$ $\geq 7.6.0 < 7.6.6$	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-2x38-48vp-w23x
fortinet.com fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2026-24858

Additional guidance fortiguard.fortinet.com/psirt/FG-IR-26-060
NVD nvd.nist.gov/vuln/detail/CVE-2026-24858
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-4712

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