CYBER ADVISORY

Wednesday, January 28, 2026 **CAL-CSIC-202601-A-012**

Fortinet Authentication Bypass Vulnerability

CWE-288	Exploited in the Wild	Bypass Authentication	SSO Login

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability impacting multiple Fortinet products. CVE-2026-24858 has a CVSS 3.1 score of 9.8 and stems from authentication bypass using an alternate path or channel (CWE-288).[1] An attacker with a FortiCloud account and registered device can gain access to devices associated with other accounts if FortiCloud SSO authentication is enabled.[2] Although FortiCloud SSO login is not enabled in default factory settings it becomes enabled when an administrator registers the device.

This vulnerability has been confirmed to be exploited in the wild and added to CISA's Known Exploited Vulnerabilities (KEV) catalog. It has been observed that attackers gained unauthorized administrative access, downloaded configuration files, and created local administrator accounts to maintain persistence.[3]

The Cal-CSIC recommends immediately following the vendor's guidance and mitigation options outlined in the FortiGuard Advisory.[4]

https://fortiguard.fortinet.com/psirt/FG-IR-26-060

Affected Products

Version	Affected
FortiAnalyzer 7.6	7.6.0 through 7.6.5
FortiAnalyzer 7.4	7.4.0 through 7.4.9
FortiAnalyzer 7.2	7.2.0 through 7.2.11
FortiAnalyzer 7.0	7.0.0 through 7.0.15
FortiManager 7.6	7.6.0 through 7.6.5
FortiManager 7.4	7.4.0 through 7.4.9
FortiManager 7.2	7.2.0 through 7.2.11
FortiManager 7.0	7.0.0 through 7.0.15

FortiOS 7.6	7.6.0 through 7.6.5
FortiOS 7.4	7.4.0 through 7.4.10
FortiOS 7.2	7.2.0 through 7.2.12
FortiOS 7.0	7.0.0 through 7.0.18
FortiProxy 7.6	7.6.0 through 7.6.4
FortiProxy 7.4	7.4.0 through 7.4.12
FortiProxy 7.2	7.2 all versions
FortiProxy 7.0	7.0 all versions

References

[1] NVD; "CVE-2026-24858"; https://nvd.nist.gov/vuln/detail/CVE-2026-24858; accessed 28 January 2026.
[2] Hacker News; "Fortinet Patches CVE-2026-24858 After Active FortiOS SSO Exploitation Detected"; https://thehackernews.com/2026/01/fortinet-patches-cve-2026-24858-after.html; accessed 28 January 2026.
[3] Cyber Press; "Fortinet Warns of Actively Exploited FortiCloud SSO Flaw (CVE-2026-24858)"; https://cyberpress.org/fortinet-actively-exploited-forticloud-sso-vulnerability-cve-2026-24858/; accessed 28 January 2026.
[4] PSIRT; "Administrative FortiCloud SSO authentication bypass"; https://fortiguard.fortinet.com/psirt/FG-IR-26-060; accessed 28 January 2026.