An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2601280226

NCSC Advisory

Critical Authentication Bypass Vulnerability in FortiOS SSO

CVE-2026-24858

28th, January 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Description

CVE ID: CVE-2026-24858

Published: 2026-01-27

Vendor: Fortinet

Product: FortiAnalyzer, FortiOS, FortiManager

CVSS Score[1]: 9.4

Products Affected

Product	Version
FortiAnalyzer	7.6.0 <= 7.6.5
FortiAnalyzer	7.4.0 <= 7.4.9
FortiAnalyzer	7.2.0 <= 7.2.11
FortiAnalyzer	7.0.0 <= 7.0.15
FortiOS	7.6.0 <= 7.6.5
FortiOS	7.4.0 <= 7.4.10
FortiOS	7.2.0 <= 7.2.12
FortiOS	7.0.0 <= 7.0.18
FortiManager	7.6.0 <= 7.6.5
FortiManager	7.4.0 <= 7.4.9
FortiManager	7.2.0 <= 7.2.11
FortiManager	7.0.0 <= 7.0.15

[1] https://www.first.org/cvss/

Impact

An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] in FortiOS, FortiManager, FortiAnalyzer 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.

By default the FortiCloud SSO login feature is not enabled in default factory settings. However, when an administrator registers the device to FortiCare from the device's GUI, unless the administrator disables the toggle switch "Allow administrative login using FortiCloud SSO" in the registration page, FortiCloud SSO login is enabled upon registration. This vulnerability has been seen exploited in the wild by two malicious FortiCloud accounts – please see the IOCs section.

Common Weakness Enumeration (CWE)[2]: CWE-288: Improper access control

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

IOCs

Category	IOCs
SSO Login User Accounts	cloud-noc@mail[.]io cloud-init@mail[.]io
Cloudflare Protected IPs	104.28.195[.]105 104.28.195[.]106 104.28.212[.]114 104.28.212[.]115 104.28.227[.]105 104.28.227[.]106 104.28.244[.]114 104.28.244[.]115
Additional IPs observed by a third party	37.1.209[.]19 217.119.139[.]50
Malicious Local Account Creation Name	audit, backup, backupadmin, deploy, itadmin, remoteadmin, secadmin, security, support, svcadmin, system
Attacker Main Operations	Download customer config file. Add an admin account to get persistence.

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Fortinet.

- https://nvd.nist.gov/vuln/detail/CVE-2026-24858
- https://www.cve.org/CVERecord?id=CVE-2026-24858
- https://fortiguard.fortinet.com/psirt/FG-IR-26-060
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-24858
- https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios