THREAT BULLETINS

Active Exploitations of an Authentication Bypass Vulnerability on Administrative FortiCloud SSO (CVE-2026-24858)

TLP:WHITE

Jan 28, 2026

On January 15, 2026, a critical **authentication bypass** vulnerability, tracked as **CVE-2026-24858**, in FortiCloud SSO was discovered. It allows unauthenticated remote attackers to gain administrative access to Fortinet devices.

Recently, the vulnerability has been observed being actively exploited in the wild and has been added to CISA's Known Exploited Vulnerabilities (KEV) Catalog on January 27, 2026.

Healthcare organizations must patch immediately or disable FortiCloud SSO to prevent unauthorized network entry and potential patient data breaches.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their level of risk from this vulnerability.

Analysis

CVE-2026-24858 is a critical **authentication bypass** vulnerability (CVSS score of 9.8) affecting multiple Fortinet products, including FortiOS, FortiManager, and FortiAnalyzer. Discovered in early 2026, it stems from an 'alternate path or channel' flaw (CWE-288) within the

FortiCloud Single Sign-On (SSO) implementation. An unauthenticated remote attacker with their own FortiCloud account and a registered device can exploit this weakness to bypass authentication and gain administrative access to other organizations' devices, provided those devices have FortiCloud SSO enabled. Unlike previous flaws, this zero-day was found to bypass initial patches released for similar SAML-related vulnerabilities in late 2025.

For the healthcare industry, this vulnerability presents a severe risk to patient data confidentiality and system availability. Health networks often rely on FortiGate firewalls to secure Electronic Health Record (EHR) databases and telehealth gateways; a successful bypass allows attackers to exfiltrate firewall configurations, create persistent local admin accounts, and potentially pivot deeper into the clinical network. In January 2026, active exploitation was observed where threat actors used automated scripts to grant themselves VPN access. Such unauthorized access could lead to ransomware deployment or the disruption of critical medical services, directly threatening patient safety and regulatory compliance (i.e., HIPAA).

To secure medical environments, organizations must immediately **upgrade to FortiOS 7.4.11**, **7.6.4**, **7.2.12**, or **higher**, as Fortinet has now required that FortiCloud SSO only function on patched versions. If patching is delayed, administrators should immediately **disable the 'admin-forticloud-sso-login'** setting and restrict administrative access to a dedicated management VLAN or trusted internal IPs using local-in policies. Finally, security teams should audit logs for unauthorized accounts (i.e., 'cloud-init@mail[.]io') and rotate all credentials, including LDAP/AD secrets, as a 'prevention-first' measure to neutralize potential persistence established by attackers.

Recommendations and Mitigations

Health-ISAC, together with the official FortiGuard PSIRT advisory (FG-IR-26-060), recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- **Upgrade Firmware Immediately:** Install the latest patched versions to restore FortiCloud SSO functionality and mitigate the vulnerability:
  - ***FortiOS:*** *7.4.11+, 7.6.6+, 7.2.13+, or 7.0.19+*
  - ***FortiManager/FortiAnalyzer:*** *7.4.10+, 7.6.6+, 7.2.12+, or 7.0.16+*
- **Restrict Administrative Access:** Implement a **local-in policy** to ensure the management interface is accessible only from a 'Management VLAN' or from specific, trusted internal IP addresses.
- **Disable Internet-Facing Management:** Ensure that HTTP/HTTPS administrative access is **disabled** on all internet-facing (WAN) interfaces.
- **Audit Administrator Accounts:** Review the device's user list for unauthorized or suspicious accounts. Known malicious accounts used in this campaign include:
  - cloud-init@mail[.]io
  - cloud-noc@mail[.]io
  - *Generic persistent names like itadmin, support, or secadmin.*
- **Review Configuration Changes:** Check for unauthorized changes to VPN settings, firewall rules, or the creation of new SSL-VPN user groups, which could serve as backdoors.
- **Rotate All Credentials:** If any indicators of compromise (IoCs) are found, treat the device as fully compromised. **Rotate all secrets**, including local admin passwords and credentials for any connected LDAP/Active Directory service accounts.
- **Restore from Clean Backup:** If tampering is suspected, wipe the device and restore the configuration from a verified backup taken prior to mid-January 2026.
- **Enable Enhanced Logging:** For HIPAA compliance and forensic readiness, ensure all administrative logins and configuration changes are forwarded to a remote, hardened syslog or FortiAnalyzer.
- **Segment Clinical Networks:** Ensure that edge firewalls are physically or logically separated from the **Medical Device (IoMT)** network to prevent lateral movement in the event of a bypass.
- **Audit SAML Implementations:** While FortiCloud SSO is the primary vector, Fortinet warns that this vulnerability affects other **SAML-based SSO** configurations. Audit all third-party identity provider integrations on your security appliances.

- **Reviewing the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

Reference(s)	fortiguard, hhs, fortinet

Sources
https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios

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

Alert ID ef1be5dc

View Alert

Share Feedback
was this helpful? |

Tags FortiCloud SSO, CVE-2026-24858, FortiCloud, Authentication Bypass

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**