Cybersecurity Awareness Bulletin

FortiCloud SSO Bypass: Authentication Vulnerability

OVERVIEW: The Mississippi Cyber Unit is reporting a critical authentication bypass vulnerability (CVE-2026-24858) affecting Fortinet products like FortiOS, FortiManager, and FortiAnalyzer when **FortiCloud Single Sign-On** (SSO) **is enabled.** Attackers with a legitimate FortiCloud account and a registered device can exploit this flaw to bypass normal authentication and gain administrative access to other customers' devices. There is evidence of active exploitation in the wild, including unauthorized logins and configuration downloads. Fortinet has released patched firmware (e.g., FortiOS 7.4.11 and equivalents) to remediate the issue and urges immediate updates. Until patches are applied, administrators are advised to disable FortiCloud SSO and review logs for suspicious activity.

Please note that the FortiCloud SSO login feature is not enabled in the default factory settings. However, when an administrator registers a device with FortiCare through the GUI, FortiCloud SSO is enabled by default unless the "Allow administrative login using FortiCloud SSO" option is turned off.

THREAT INTELLIGENCE:

The vulnerability stems from an alternate authentication path (CWE-288) and has a high severity score (CVSS 9.4/9.8), meaning it can be exploited remotely with no privileges required. The attacker's main operations have consisted of downloading the customer config file and/or adding an admin account to attain persistence.

User Accounts: The actor has been observed to have logged in with the following user accounts (expect these addresses may change in the future, as action has been taken to neutralize these accounts)

- cloud-noc@mail.io
- cloud-init@mail.io
- heltaylor.12@tutamail.com
- support@openmail.pro

IP Addresses: The actor has been observed to log in via multiple IP addresses and appears to have switched to use Cloudflare protected IP:

- 104.28.244.115
- 104.28.212.114
- 104.28.212.115
- 104.28.195.105
- 104.28.195.106
- 104.28.227.106
- 104.28.227.105
- 104.28.244.114
- 163.61.198.15
- 104.28.244.116
- 38.54.6.28

Admin Accounts: Following authentication via SSO, it has been observed that the actor creates a local admin account with one of the following names. *This has changed through analysis, so Fortinet recommends reviewing all admin accounts to look for any unexpected entries*.

- Audit
- Backup
- Itadmin
- Secadmin
- Support
- Backupadmin
- Deploy
- Remoteadmin
- Security
- Svcadmin
- System
- Adccount

AFFECTED SYSTEMS:

The following versions are affected:

- Affected from **7.6.0** through **7.6.4**
- Affected from **7.4.0** through **7.4.12**
- Affected from **7.2.0** through **7.2.15**
- Affected from **7.0.0** through **7.0.22**

RECOMMENDATIONS:

The Mississippi Cyber Unit provides the following recommendations:

- **Apply Updates:** Immediately ensure your device is running the latest release (7.6).
- **Disable FortiCloud SSO Logins Workaround:** Navigate to System -> Settings and toggle Allow administrative login using FortiCloud SSO to Off.
- **Restrict Administrative Access:** Do not allow unrestricted administration of any edge network device via the internet.
- **Monitor for Incident Updates**

Resources

The links below contain information on this advisory and are not maintained by the Mississippi Office of Homeland Security (MOHS). Links to are provided for the reader’s convenience and do not represent an endorsement by MOHS or the Department of Public Safety (DPS) of any commercial or private issues, products, or services.

- PSIRT | FortiGuard Labs
- Analysis of Single Sign-On Abuse on FortiOS | Fortinet Blog
- CVE Record: CVE-2026-24858
- Analysis of Single Sign-On Abuse on FortiOS | Fortinet Blog

Report Suspicious Activity

Stakeholders can report suspicious activity to ms-cyber@dps.ms.gov or by phone at 601-933-7200; or 1-888-4SAFE-MS. This email is not monitored 24 hours a day, and if there is an emergency, please dial 911. Citizens should always call local law enforcement.

(U) Standing Information Needs (SINS) Supported

HSEC-1.1: Cyber Attacks and Exploitation

MS-14000-09: Cyber Crime