TLP:CLEAR【全分野】

別紙

2026 年 1 月 28 日

内閣官房　国家サイバー統括室
対処調整・官民連携等ユニット

Fortinet 製品の深刻な脆弱性(CVE-2026-24858)について
(注意喚起)

1. 対象ソフトウェア

・FortiOS　　7.6 系、7.4 系、7.2 系、7.0 系
・FortiProxy　7.6 系、7.4 系
・FortiManager　7.6 系、7.4 系、7.2 系、7.0 系
・FortiAnalyzer 7.6 系、7.4 系、7.2 系、7.0 系
※なお、FortiProxy 7.2 系及び 7.0 系については後継バージョンへの移行が推奨されています

2. 脆弱性悪用による影響等

対象ソフトウェアにおいて、FortiCloud SSO ログイン機能を有効化している場合、FortiCloud アカウントと登録済みデバイスを持つ攻撃者によって、FortiCloud アカウントに登録されている組織のデバイスにログインされる恐れがあります。

3. 悪用

開発元において、脆弱性を悪用した攻撃が発生し、被害組織のデバイス上でローカル管理者アカウントが作成されたことが確認されています（参考 URL)。

4. 対応

対象ソフトウェアの最新のアップデートの適用を強く推奨します。また、手動で SSO ログイン機能を無効化することで脆弱性の悪用を回避できます（参考 URL)。

5. その他

開発元より、現時点で脆弱なバージョンを実行しているデバイスからの FortiCloud SSO ログインをサポートしない設定を行っており、ユーザー側で SSO ログインを無効にする必要はないとされています（参考 URL)。一方、開発元の対応によらず、4. 対応に記載した内容を確実に実施していただくことが必要です。

参考 URL
- Administrative FortiCloud SSO authentication bypass (Fortinet 社)
  https://fortiguard.fortinet.com/psirt/FG-IR-26-060