2026 年 01 月 28 日
株式会社ネットワールド

複数の Fortinet 製品の FortiCloud の SSO ログイン認証バイパスの脆弱性について

Fortinet 社の PSIRT(Product Security Incident Response Team)より Critical として、 以下の情報が公開されましたので、以下の通りご報告させていただきます。

概要:
FortiOS、FortiManager、FortiAnalyzer、FortiProxy、FortiWeb における代替パスまたはチャネルを用いた認証バイパスの脆弱性［CWE-288］により、FortiCloud アカウントと登録済みデバイスを持つ攻撃者が、FortiCloud SSO 認証が有効になっているデバイスに、別のアカウントで登録されているデバイスにログインできる可能性があります。

FortiCloud SSO ログイン機能は、工場出荷時のデフォルト設定では無効になっていますのでご注意ください。ただし、管理者がデバイスの GUI からデバイスを FortiCare に登録する場合、登録ページで「FortiCloud SSO を使用した管理者ログインを許可する」トグルスイッチを無効にしない限り、登録時に FortiCloud SSO ログインが有効になります。

この脆弱性は、悪意のある 2 つの FortiCloud アカウントによって悪用されていることが確認され、2026 年 1 月 22 日にロックアウトされました。Fortinet は、お客様をさらなる悪用から保護するため、2026 年 1 月 26 日に FortiCloud 側で FortiCloud SSO を無効化しました。 2026 年 1 月 27 日に再有効化されましたが、脆弱性のあるバージョンを実行しているデバイスからのログインはサポートされなくなりました。そのため、FortiCloud SSO 認証を機能させるには、下記の最新バージョンにアップグレードする必要があります。

CVE ID：
CVE-2025-64446

影響：
不適切なアクセス制御

影響を受けるバージョン及び対策

FortiManager Cloud、FortiAnalyzer Cloud、FortiGate Cloud は影響を受けません。
FortiCloud ではなくカスタム IdP を SSO に使用している環境（FortiAuthenticator をカスタム IdP として使用している環境を含む）は影響を受けません。
以下の製品は調査中です：FortiSwitch Manager

モデル・バージョン	対象バージョン	対策
FortiAnalyzer 7.6	7.6.0 ～ 7.6.5	7.6.6 以上にアップグレードしてください
FortiAnalyzer 7.4	7.4.0 ～ 7.4.9	7.4.10 以上にアップグレードしてください
FortiAnalyzer 7.2	7.2.0 ～ 7.2.11	7.2.12 以上にアップグレードしてください
FortiAnalyzer 7.0	7.0.0 ～ 7.0.15	7.0.16 以上にアップグレードしてください
FortiAnalyzer 6.4	影響なし	該当なし
FortiManager 7.6	7.6.0 ～ 7.6.5	7.6.6 以上にアップグレードしてください
FortiManager 7.4	7.4.0 ～ 7.4.9	7.4.10 以上にアップグレードしてください
FortiManager 7.2	7.2.0 ～ 7.2.11	7.2.13 以上にアップグレードしてください
FortiManager 7.0	7.0.0 ～ 7.0.15	7.0.16 以上にアップグレードしてください
FortiManager 6.4	影響なし	該当なし
FortiOS 7.6	7.6.0 ～ 7.6.5	7.6.6 以上にアップグレードしてください
FortiOS 7.4	7.4.0 ～ 7.4.10	7.4.11 以上にアップグレードしてください
FortiOS 7.2	7.2.0 ～ 7.2.12	7.2.13 以上にアップグレードしてください
FortiOS 7.0	7.0.0 ～ 7.0.18	7.0.19 以上にアップグレードしてください
FortiOS 6.4	影響なし	該当なし
FortiProxy 7.6	7.6.0 ～ 7.6.4	7.6.6 以上にアップグレードしてください
FortiProxy 7.4	7.4.0 ～ 7.4.12	7.4.13 以上にアップグレードしてください
FortiProxy 7.2	7.2 全てのバージョン	修正バージョンへ移行してください
FortiProxy 7.0	7.0 全てのバージョン	修正バージョンへ移行してください
FortiWeb 8.0	8.0.0 ～ 8.0.3	8.0.4 以上にアップグレードしてください
FortiWeb 7.6	7.6.0 ～ 7.6.6	7.6.7 以上にアップグレードしてください
FortiWeb 7.4	7.4.0 ～ 7.4.11	7.4.12 以上にアップグレードしてください
FortiWeb 7.2	影響なし	該当なし
FortiWeb 7.0	影響なし	該当なし

回避策

FortiCloud SSO 認証は、脆弱なバージョンを実行しているデバイスからのログインをサポートしなくなりました。
そのため、現時点ではクライアント側で FortiCloud SSO ログインを無効にする必要はありません。ただし、以下の手順で無効化することも可能です。

・FortiOS および FortiProxy の場合：
「システム」→「設定」→「FortiCloud SSO を使用した管理者ログインを許可する」をオフにします。または、CLI コマンドラインで以下のコマンドを入力します。

```
config system global
    set admin-forticloud-sso-login disable
end
```

・FortiManager および FortiAnalyzer の場合：
「システム設定」→「SAML SSO」→「管理者に FortiCloud でのログインを許可する」をオフにします。または、CLI コマンドラインで以下のコマンドを入力します。

```
config system saml
    set forticloud-sso disable
end
```

侵害の兆候

・SSO ログインユーザーアカウント
攻撃者は以下のユーザーアカウントでログインしたことが確認されています。

cloud-noc@mail.io
cloud-init@mail.io

これらのアカウントを無効化するための措置が講じられたため、これらのアドレスは今後変更される可能性があります。

・IP アドレス
攻撃者は複数の IP アドレスでログインしたことが確認されており、Cloudflare で保護された IP アドレスを使用するように切り替えたようです。

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

・Fortinet 以外の第三者によって観測された追加の IP アドレス：

37[.]1.209.19
217[.]119.139.50

・悪意のあるローカルアカウントの作成
SSO 認証後、攻撃者は以下のいずれかの名前でローカル管理者アカウントを作成することが確認されています。
これは当社の分析により変更されているため、フォーティネットはすべての管理者アカウントを確認し、予期しないエントリがないか確認することを推奨します。

audit
backup
itadmin
secadmin
support
backupadmin
deploy
itadmin
remoteadmin
security
svcadmin
system

攻撃者の主な操作：
・顧客の設定ファイルをダウンロードする
・管理者アカウントを追加して永続性を確保する

詳細は以下をご参照ください。
https://fortiguard.fortinet.com/psirt/FG-IR-26-060

以上