2025 年 12 月 10 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、FortiWeb、FortiProxy、およびFortiSwitchManagerにおける暗号署名の不適切な検証に関する脆弱性[CWE-347]により、デバイスでFortiCloud SSOログイン認証が有効になっている場合、認証されていない攻撃者が細工されたSAMLメッセージを介してFortiCloud SSOログイン認証をバイパスできる可能性があります。

CVE ID：
CVE-2025-59718 / CVE-2025-59719

影響：
不適切なアクセス制御

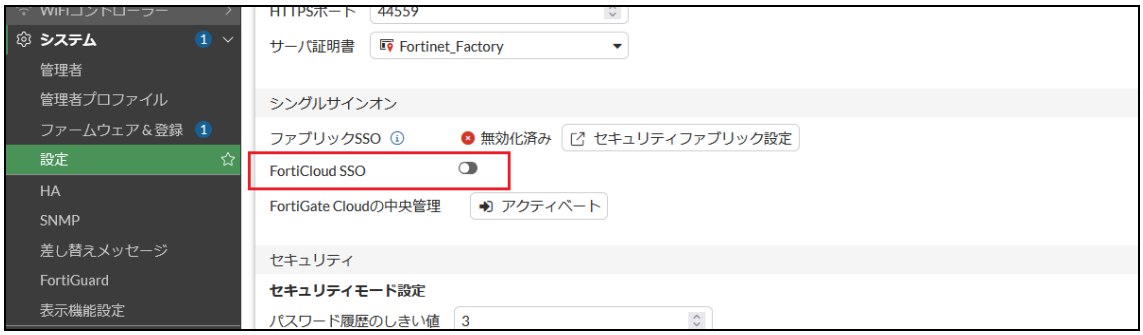
バージョン	対象バージョン	対策バージョン
FortiOS v7.6	v7.6.0～v7.6.3	v7.6.4以降へのアップグレードしてください
FortiOS v7.4	v7.4.0～v7.4.8	v7.4.9以降へのアップグレードしてください
FortiOS v7.2	v7.2.0～v7.2.11	v7.2.12以降へのアップグレードしてください
FortiOS v7.0	v7.0.0～v7.0.17	v7.0.18以降へのアップグレードしてください
FortiOS v6.4	影響なし	該当しません
FortiProxy v7.6	v7.6.0～v7.6.3	v7.6.4以降へのアップグレードしてください
FortiProxy v7.4	v7.4.0～v7.4.10	v7.4.11以降へのアップグレードしてください
FortiProxy v7.2	v7.2.0～v7.2.14	v7.2.15以降へのアップグレードしてください
FortiProxy v7.0	v7.0.0～v7.0.21	v7.0.22以降へのアップグレードしてください
FortiSwitchManager v7.2	v7.2.0～v7.2.6	v7.2.7以降へのアップグレードしてください
FortiSwitchManager v7.0	v7.0.0～v7.0.5	v7.0.6以降へのアップグレードしてください
FortiWeb v8.0	v8.0.0	v8.0.1以降へのアップグレードしてください
FortiWeb v7.6	v7.6.0～v7.6.4	v7.6.5以降へのアップグレードしてください
FortiWeb v7.4	v7.4.0～v7.4.9	v7.4.10以降へのアップグレードしてください
FortiWeb v7.2	影響なし	該当しません
FortiWeb v7.0	影響なし	該当しません

回避策：
FortiCloud SSOログイン機能は、工場出荷時のデフォルト設定では有効になっていません。

ただし、管理者がデバイスのGUIからデバイスをFortiCareに登録する際、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。

脆弱性のあるバージョンでこの脆弱性の影響を受けないようにするには、影響を受けないバージョンにアップグレードするまで、FortiCloudログイン機能（有効になっている場合）を一時的に無効にしてください。

FortiCloudログインを無効にするには、「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で以下のコマンドを入力します。

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

詳細は以下をご参照ください。
https://fortiguard.fortinet.com/psirt/FG-IR-25-647

以上