2025 年 5 月 14 日

お客様各位

株式会社日立ソリューションズ
Fortinet 製品ユーザサポート

【脆弱性】FortiOS の TACACS+における認証バイパスの脆弱性(CVE-2025-22252)について

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

この度 Fortinet 社より、深刻度の高い脆弱性として、FortiOS などに関する脆弱性(CVE-2025-22252)がアナウンスされています。本脆弱性の影響を受けるバージョンをご利用のお客様におかれましては、対策済み OS へのバージョンアップや回避策の適用について、ご検討をお願いいたします。

敬具

記

1. 事象の概要

FortiOS の TACACS+認証において、重要な機能に対する認証の欠如[CWE-306]があり、TACACS+の Authentication Type(認証タイプ)を ASCII で利用している場合、既存の管理者アカウントを知っている攻撃者が、認証をバイパスしてデバイスにアクセスできる可能性があります。

本脆弱性は TACACS+の認証タイプを ASCII で利用している場合のみ影響を受けます。FortiOS のデフォルト設定では、認証タイプに ASCII は設定されていません。

詳細、最新の情報については Fortinet 社から発表されています以下セキュリティアドバイザリ(PSIRT Advisories)をご覧ください。

TACACS+ authentication bypass
<https://fortiguard.fortinet.com/psirt/FG-IR-24-472>

2. 該当製品と対策バージョン

弊社取り扱い済みの製品・バージョンにて、脆弱性の影響を受けるバージョン、及び対策バージョンは以下の通りです。

項	メジャーバージョン	影響を受ける バージョン	対策 バージョン	備考
1	FortiOS 7.6 系	7.6.0	7.6.1 以降	FortiOS 7.6 系は弊社未リリースのバージョン
2	FortiOS 7.4 系	7.4.4～7.4.6	7.4.7 以降	
3	FortiOS 7.2 系	なし	—	
4	FortiOS 7.0 系	なし	—	
5	FortiOS 6.4 系	なし	—	EOS 済みバージョン

3. 回避策

TACACS+の認証タイプで ASCII 以外を利用することにより回避可能です。
以下に CLI での設定例を示します。

authen-type に pap、mschap または chap を指定

```
config user tacacs+
    edit "TACACS-SERVER"
        set server <IP address>
        set key <string>
        set authen-type [pap, mschap, chap]
        set source-ip <IP address>
    next
end
```

または、authen-type にデフォルト(auto)を設定

```
config user tacacs+
    edit "TACACS-SERVER"
        set server <IP address>
        set key <string>
        unset authen-type
        set source-ip <IP address>
    next
end
```

4. OS ファイルの入手方法

OS ファイルは、弊社サポートからご提供しております。対象機器のシリアル番号 (S/N)と共に、現在のバージョン、バージョンアップ先のバージョンをご連絡ください。

5. Fortinet 社セキュリティアドバイザリ

Fortinet 社では、脆弱性情報を以下、FortiGuard Labs PSIRT Advisories で公開しています。最新の脆弱性情報は以下サイトをご覧頂き、適時ご利用環境の対策をいただきますようお願いします。

尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また内容等については、弊社サポートではお答えいたしかねます。予めご了承ください。

PSIRT Advisories は RSS 配信も行われていますので、合わせてご活用ください。

FortiGuard Labs PSIRT Advisories
<https://www.fortiguard.com/psirt>

FortiGuard Labs RSS Feeds
<https://www.fortiguard.com/rss-feeds>

以上