2025 年 5 月 14 日

お客様各位

パナソニック ソリューションテクノロジー株式会社

# フォーティネット社脆弱性情報(FG-IR-24-472)(CVE-2025-22252)

平素は格別のご高配を賜り、厚くお礼申し上げます。

Fortinet 社より、下記の重大な脆弱性問題が発表されております。
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ついては、以下の対策のご対応をお願いいたします。

◆CVE 番号
CVE-2025-22252　CVSSv3 Score：9.0　重要度：Critical

◆影響
FortiOS、FortiProxy、および FortiSwitchManager の TACACS+ において、認証にリモートの TACACS+ サーバを使用するように設定されていますが、それ自体が ASCII 認証を使用するように設定されており、重要な機能に対する認証が欠落する脆弱性 [CWE-306]があり、既存の管理者アカウントを知っている攻撃者が、認証バイパスを介して有効な管理者としてデバイスにアクセスできる可能性があります。

◆対象製品/影響を受けるバージョン/対策

| 対象製品 | 影響を受ける<br>対象バージョン | 対策(下記バージョンへの<br>アップグレードを実施してください |
|---|---|---|
| FortiOS 7.6 | 7.6.0 | 7.6.1 以降 |
| FortiOS 7.4 | 7.4.4 ~ 7.4.6 | 7.4.7 以降 |
| FortiOS 7.2 | 影響なし | 該当なし |
| FortiOS 7.0 | 影響なし | 該当なし |
| FortiOS 6.4 | 影響なし | 該当なし |
| FortiProxy 7.6 | 7.6.0 ~ 7.6.1 | 7.6.2 以降 |
| FortiProxy 7.4 | 影響なし | 該当なし |
| FortiProxy 7.2 | 影響なし | 該当なし |
| FortiProxy 7.0 | 影響なし | 該当なし |
| FortiProxy 2.0 | 影響なし | 該当なし |

| | | |
|---|---|---|
| FortiSwitchManager 7.2 | 7.2.5 | 7.2.6 以降 |
| FortiSwitchManager 7.0 | 影響なし | 該当なし |

◆回避策
別の認証方法を使用します。

```
config user tacacs+
    edit "TACACS-SERVER"
        set server <IP address>
        set key <string>
        set authen-type [pap, mschap, chap]　←ascii 以外を選択します
        set source-ip <IP address>
    next
end
```

又は

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

デフォルトでは、ASCII 認証は使用されません。

本内容は 2025 年 5 月 14 日時点のものとなります。最新の情報は以下のメーカーサイトよりご確認をお願いいたします。

◆Fortinet FortiGuard Labs
TACACS+ authentication bypass
https://www.fortiguard.com/psirt/FG-IR-24-472