TLP:CLEAR【全分野】

別紙

2024 年 2 月 9 日

内閣官房　内閣サイバーセキュリティセンター
重要インフラグループ

# Fortinet 製品の深刻な脆弱性(CVE-2024-21762)について(注意喚起)

1. 対象ソフトウェア
・FortiOS　6.0.x、6.2.0 から 6.2.15、6.4.0 から 6.4.14、7.0.0 から 7.0.13、7.2.0 から 7.2.6、7.4.0 から 7.4.2

2. 脆弱性悪用による影響等
対象ソフトウェアを使用しているネットワーク機器に対して、攻撃者による任意のコード実行等の恐れがあります。

3. 深刻度
ソフトウェアの開発元が深刻度「Critical」(5 段階中、最高)に分類する脆弱性が含まれます。

4. 悪用
脆弱性を悪用した攻撃が発生している可能性があることを開発元が公表しています。

5. 対応
対象ソフトウェアの最新のバージョンへの更新を強く推奨します。更新を直ちに実施できない場合は、緩和策(6.参照)や監視の強化等を検討してください。

6. その他
SSL-VPN 機能を無効にしている場合、本脆弱性の影響は軽減されますが、ソフトウェアの健全性維持の観点からも、最新バージョンへの更新を強く推奨します。ソフトウェアサポートが終了している機器を使用している場合は、直ちに最新バージョンへの更新をしてください。

参考 URL
- FortiOS - Out-of-bound Write in sslvpnd (Fortinet)
  https://www.fortiguard.com/psirt/FG-IR-24-015
- Fortinet 製 FortiOS SSL VPN の脆弱性対策について(CVE-2024-21762)
  https://www.ipa.go.jp/security/security-alert/2023/alert20240209.html