FUKUOKA POLICE 70th ANNIVERSARY

福岡県警察からのお願い

令和７年1月 号外

FortiOS及びFortiProxyに脆弱性

Fortinet社は,同社のネットワーク機器のオペレーティングシステム「FortiOS」及びWebプロキシ製品「FortiProxy」に重大な脆弱性（CVE-2024-55591）があると公表しました。

本脆弱性はCVSSスコア9.8（最大10.0）と評価されており極めて深刻度の高い脆弱性です。

本脆弱性を放置すると、遠隔の攻撃者が細工したパケットを機器に送信することで、認証を回避して管理者権限を取得される可能性があります。

Q　本脆弱性を悪用され、悪意を持った第三者に管理者権限を取得されると・・・？

➢　攻撃者は機密情報の盗難や改ざん、システムの破壊活動、ランサムウェアをはじめとしたマルウェアの感染・拡散等、様々なことが実行可能となり、システム全体が脅威に晒されます。

■ 公開された脆弱性情報（CVE-2024-55591）

製品	影響を受けるバージョン	脆弱性が修正されたバージョン
FortiOS 7.6	影響なし	-
FortiOS 7.4	影響なし	-
FortiOS 7.2	影響なし	-
FortiOS 7.0	7.0.0から7.0.16	7.0.17以降
FortiOS 6.4	影響なし	-
FortiProxy 7.6	影響なし	-
FortiProxy 7.4	影響なし	-
FortiProxy 7.2	7.2.0から7.2.12	7.2.13以降
FortiProxy 7.0	7.0.0から7.0.19	7.0.20以降
FortiProxy 2.0	影響なし	-

■ 対策・回避策

Fortinet社が提供している脆弱性が修正されたバージョンに更新してください。また回避策として、
・機器のHTTP/HTTPSを使用した管理機能を無効化
・機器の管理機能に対する接続を、信頼できるアクセス元IPアドレスからのみに制限
が示されています。

※詳細については、フォーティネット社のアドバイザリを参照してください。
https://www.fortiguard.com/psirt/FG-IR-24-535

ランサムウェアや不正アクセス等のサイバー事案の被害に遭われた場合は、最寄りの警察署に通報・相談してください。

◆ **万が一、サイバー犯罪の被害に遭われた方は、管轄の警察署まで通報してください。**

◆ **福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などを、X（旧Twitter）やホームページに掲載していますので、ぜひご覧ください。**

【X】（旧Twitter）　【ホームページ】