サイバーセキュリティ パートナーシップだより

R6-19

Fortinet社製品を利用している皆様へ

FortiManagerの脆弱性情報が公開されました(CVE-2024-47575)

公開された脆弱性が放置されたままだと、攻撃者に悪用され、外部から任意のコードまたはコマンドを実行される可能性があります。

【影響を受けるシステム／バージョン】

- **Forti Manager : 7.6.0、7.4.0～7.4.4、 7.2.0 ～ 7.2.7、7.0.0 ～ 7.0.12、6.4.0 ～ 6.4.14、6.2.0～6.2.12**
- **Forti Manager Cloud : 7.4.1 ～ 7.4.4、7.2.1 ～ 7.2.7、7.0.1 ～ 7.0.12、6.4系の全バージョン**
- **Forti Analyzer : 1000E、1000F、2000E、3000E、3000F、3000G、3500E、3500F、3500G、3700F、3700G、3900E**

※　上記製品は、Fortinet社製のVPN機器やUTM機器等を一元管理したり、ログ等を集中管理するのに使用される製品です。

＝＝

【 推 奨 さ れ る 対 策 】

■　**脆弱性が修正されたバージョンに更新**

■　修正されたバージョンへの更新が困難な場合は下記のFortinet社のページに記載された回避策の適用を検討

＝＝

※　最新の情報及び詳細はFortinet社のページ
https://fortiguard.fortinet.com/psirt/FG-IR-24-423 を参照

ランサムウェア感染や不正アクセス等による情報漏洩の被害防止策として、まずは自社がどこのメーカーのネットワーク機器やセキュリティ製品を使っているか再確認していただき、該当の製品をお使いの場合は、上記対策を行ってください。業務を請け負う保守業者の皆さまにおかれましても、今一度ご確認をお願いします。