サイバーニュース

令和５年号外
奈良県警察本部
サイバー犯罪対策課

御社のシステムは大丈夫ですか？

重要!

新型コロナウイルス感染症の拡大を受け、**VPN機器**を導入し、テレワークを取り入れた事業者の方も多いと思います。

しかしその一方で、**VPN機器の脆弱性**を狙ったランサムウェア攻撃により被害を受ける企業・団体等が後を絶たず、**VPN機器の脆弱性対策**が求められています！

下記の製品を使用されている方は、導入している**VPN機器のシステム・バージョン等**をご確認ください！

VPN･･･Virtual Private Networkの略
インターネット回線を利用した専用のネットワーク※テレワーク等で利用

Fortinet社製品を利用している皆様へ

FortiOS及びFortiProxyの脆弱性情報が公開されました(CVE-2023-25610)

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を実行されたり、ＤｏＳ攻撃（サービス拒否攻撃）を受け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 OS　：7.2.0～7.2.3、7.0.0 ～ 7.0.9、6.4.0 ～ 6.4.11、6.2.0 ～ 6.2.12、6.0系の全バージョン
- Forti Proxy　：7.2.0 ～ 7.2.2、7.0.0 ～ 7.0.8、2.0.0 ～ 2.0.11、1.2系の全バージョン、1.1系の全バージョン
- FortiOS-6K7K: 7.0.5、6.4.10、6.4.8、6.4.6、6.4.2、6.2.12、6.2.11、6.2.10、6.2.9、6.2.7、6.2.6、6.2.4

注意

お使いのバージョンをご確認ください！

【推奨される対策】

- 脆弱性が修正されたバージョンに更新する。

【リスク緩和策】

- HTTP及びHTTPS接続を使用した管理インタフェースを無効にする。
- 管理インタフェースにアクセスできるIPアドレスを制限する。

※　詳細はFortinet社のページ
（https://www.fortiguard.com/psirt/FG-IR-23-001）を参照

もし被害に遭った場合は、
奈良県警察本部サイバー犯罪対策課に相談して下さい！
連絡先　0742-23-0110

ランサムウェアに関する詳細な情報はこちらからご確認ください

サイバーニュース
（ランサムウェアについて）