サイバー警察局便り

Cyber Police Agency Letter Vol.2

Fortinet社製品を利用している方へ

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

【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社のウェブサイト（https://www.fortiguard.com/psirt/FG-IR-23-001）を確認してください

被害に遭った場合は、最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口に通報・相談してください！

都道府県警察本部のサイバー犯罪相談窓口はこちら⇒
https://www.npa.go.jp/cyber/soudan.html

警察庁 National Police Agency

サイバー犯罪対策トップ
https://www.npa.go.jp/cyber/index.html