

Fortinet社製品を利用している皆様へ
～システム担当者や管理委託先にご確認ください～

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、D o S 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ーフェースを無効にする。
- 管理インター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、
サイバー犯罪対策課に相談して下さい！
<https://www.pref.aichi.jp/police/anzen/cyber>
(052)-951-1611 内線3345～3347

