令和４年10月13日

MiCS
みやざきサイバーセキュリティ
宮崎県企業・警察サイバーセキュリティ連携協議会

Fortinet社製品の脆弱性

警察庁では、Fortinet社が提供する製品「FortiOS」、「FortiProxy」、「FortiSwitch Manager」について脆弱性が存在し既に悪用されていることから更新プログラムの適用を呼びかけています。

１　脆弱性の概要

同脆弱性はCVE-2022-40684（CVSSスコア：9.6）であり、当該脆弱性を悪用されることにより、認証資格を持たない攻撃者が特別に細工されたhttp・httpsリクエストを介して管理インターフェイスで操作を実行できる可能性があります。

影響を受ける製品は以下のとおりです。

・FortiOS：v7.0.0~7.0.6、v7.2.0~7.2.1
⇒7.0.7、7.2.2へバージョンアップ等を推奨

・FortiProxy：v7.0.0~7.0.6、v7.2.0
⇒7.0.7、7.2.1へバージョンアップ等を推奨

・FortiSwitchManger：v7.0.0、v7.2.0
⇒7.2.1へバージョンアップ等を推奨

２　対策方法

● 更新プログラムの適用※。
● 更新プログラムの適用ができない場合、http/https管理インターフェースの無効化又はアクセスできるIPアドレスの制限を実施。
● 被害発生時には警察にも相談する。
※ 参考リンク先
【Fortinet】https://www.fortiguard.com/psirt/FG-IR-22-377
【JPCERT】https://www.jpcert.or.jp/at/2022/at220025.html

３　参考

今後、Hrizon3 Attack Teamの研究者が解説や実証コードを公開することが予定されており、更に悪用される可能性が高い脆弱性となります。