2022 年 10 月 12 日

お客様各位

株式会社日立ソリューションズ
Fortinet 製品ユーザサポート

【脆弱性】FortiOS における認証バイパスの脆弱性(CVE-2022-40684)について

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

この度 Fortinet 社より、深刻度の高い脆弱性として、FortiOS の管理インターフェースへのアクセスにおける認証バイパスの脆弱性(CVE-2022-40684)がアナウンスされています。本脆弱性の影響を受けるバージョンをご利用のお客様は、対策済み OS へのバージョンアップ、若しくは回避策・緩和策の適用について、ご検討をお願いいたします。

敬具

記

1. 事象の概要

FortiOS において、管理インターフェースへのアクセス時の認証がバイパス可能となる脆弱性が見つかりました。これにより、攻撃者が細工した HTTP/HTTPS リクエストを FortiGate の管理インターフェースに送信することにより、管理インターフェースアクセス時の認証が行われなくなる可能性があります。

Fortinet 社からは、既にこの脆弱性を悪用した攻撃が確認されていること、および緊急での対処が必要である旨が、アナウンスされています。

詳細、最新の情報については Fortinet 社から発表されています以下セキュリティアドバイザリ(PSIRT Advisories)をご覧ください。

FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface
<https://www.fortiguard.com/psirt/FG-IR-22-377>

2. 該当製品と対策バージョン

脆弱性の影響を受けるバージョン、及び対策バージョンは以下の通りです。
影響を受けるバージョンをご利用中の場合は、対策済み OS へのバージョンアップをお願いいたします。

項	メジャーバージョン	影響を受けるバージョン	対策バージョン	備考
1	FortiOS 7.2 系	7.2.0 ～ 7.2.1	7.2.2 以降	弊社からは未リリースのバージョンです。
2	FortiOS 7.0 系	7.0.0 ～ 7.0.6	7.0.7(※)以降	7.0.0 および 7.0.1 は弊社から未リリースのバージョンです。
3	FortiOS(6000 シリーズ) 7.0 系	7.0.5	－	弊社からは未リリースのバージョンです。

※ 2022 年 10 月 11 日に弊社からリリース済です。

3. 回避策および緩和策

脆弱性の回避策と緩和策は以下の通りです。なお、緩和策により IP アドレスを制限した後も、該当 IP アドレスからのアクセスには脆弱性が残るため、早急に対策バージョンへのアップグレードの検討をお願いいたします。

回避策

FortiGate の管理インターフェースにおいて、HTTP/HTTPS によるアクセスを無効化することにより、本脆弱性の回避可能です。なお、本回避策を適用すると、WebUI を使用した管理アクセスが出来なくなります。

緩和策

FortiGate の管理インターフェースへのアクセス元の IP アドレスを制限することにより、本脆弱性の影響の緩和が可能です。

FortiGate の管理インターフェースへのアクセス元の IP アドレスの制限方法については、セキュリティアドバイザリ掲載の Workaround をご覧ください。

4. OS ファイルの入手方法

バージョンアップは、対象機器がインターネットに接続している場合は、GUI で OS のダウンロード、及びバージョンアップを行うことができます。

OS ファイルがご入用の場合は、弊社サポートからご提供しております。対象機器のシリアル番号（S/N）と共に、現在のバージョン、バージョンアップ先のバージョンをご連絡ください。

5. Fortinet 社セキュリティアドバイザリ

Fortinet 社では、脆弱性情報を以下、FortiGuard Labs PSIRT Advisories で公開しています。最新の脆弱性情報は以下サイトをご覧頂き、適時ご利用環境の対策をいただきますようお願いします。

尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また内容等については、弊社サポートではお答えいたしかねます。予めご了承ください。

PSIRT Advisories は RSS 配信も行われていますので、合わせてご活用ください。

FortiGuard Labs PSIRT Advisories
<https://www.fortiguard.com/psirt>

FortiGuard Labs RSS Feeds
<https://www.fortiguard.com/rss-feeds>

以上