2024 年 10 月 31 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】FortiManager 機能における認証バイパスの脆弱性(CVE-2024-47575)について(第二報)

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、FortiManager 機能の認証に関する脆弱性(CVE-2024-47575)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におかれましては、対策済み OS へのバージョンアップや回避策の適用について、ご検討をお願いいたします。

※太字箇所が、第二報での追記もしくは更新箇所となっています。

敬具

記

1. 事象の概要

FortiManager 機能において、重要な機能に対する認証の欠如[CWE-306]があり、外部の認証されていない攻撃者に、許可されていないコードやコマンドを実行される可能性があります。

Fortinet 社は、本脆弱性を悪用した攻撃が起きている可能性があることをアナウンスしています。

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。

Missing authentication in fgfmsd
<https://fortiguard.fortinet.com/psirt/FG-IR-24-423>

2. 該当製品と対策バージョン

・FortiManager

弊社取り扱い済みの製品・バージョンにて、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。

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	FortiManager 7.4 系	7.4.4 以前	7.4.5 以降	弊社からは 10/25(金)に**リリース済**
2	FortiManager 7.2 系	7.2.7 以前	7.2.8 以降	弊社からは 10/25(金)に**リリース済**
3	FortiManager 7.0 系	7.0.12 以前	7.0.13 以降	**弊社からは 10/31(木)にリリース済**
4	FortiManager 6.4 系	6.4.14 以前	6.4.15 以降	**弊社からは 10/31(木)にリリース済**
5	FortiManager 6.2 系	6.2.12 以前	6.2.13 以降	**弊社からは 10/31(木)にリリース済**

・FortiAnalyzer

FortiAnalyzer においても、以下のすべての条件に該当する場合は、本脆弱性の影響を受けます。

・FortiAnalyzer-1000E/1000F/2000E/3000G/3700F のいずれかを利用している

・FortiAnalyzer における FortiManager 機能を有効にしている(以下の設定を行っている)

```
config system global
    set fmg-status enable
end
```

・1 つ以上のインタフェースで fgfm サービスを有効にしている

3. 回避策

FortiManager 7.4.3 以降、7.2.5 以降、7.0.12 以降については、以下の設定を行うことにより、不明なデバイスによる登録要求を拒否できます。

```
config system global
    set fgfm-deny-unknown enable
end
```

注意：上記設定を行っている場合、FortiManager のデバイスリストに FortiGate のシリアル番号が登録されていない場合、FortiGate のデプロイ時のデバイスの登録が行えなくなります。

FortiManager において、「FortiAnalyzer 機能」を有効にしている場合は、以下の設定により、syslog 経由での不明なデバイスの追加要求を拒否してください。

```
config system global
    set detect-unregistered-log-device disable
end
```

また、FortiGate のシグネチャのアップデートや Web フィルタリングが有効となっている場合は、以下の設定により、FSD(FortiGuard Distribution Servers)経由での不明なデバイスによるアクセスを拒否してください。

```
config fmupdate fds-setting
    set unreg-dev-option ignore
end
```

上記以外の軽減策については、セキュリティアドバイザリを参照してください。

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