2024 年 2 月 13 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 の fgfmd におけるフォーマット文字列に関する脆弱性(CVE-2024-23113)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、FortiOS の fgfmd におけるフォーマット文字列に関する脆弱性(CVE-2024-23113)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

FortiOS の fgfmd デーモンにおいてフォーマット文字列に関する脆弱性があり、外部からの認証されていない攻撃者に、悪意を持って細工したリクエストを介して、任意のコードやコマンドが実行される可能性があります。

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 - Format String Bug in fgfmd
<https://www.fortiguard.com/psirt/FG-IR-24-029>

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 7.4 系	7.4.0 ～ 7.4.2	7.4.3 以降	7.4 系は弊社未リリースです
2	FortiOS 7.2 系	7.2.0 ～ 7.2.6	7.2.7 以降	2024/2/9 リリース済
3	FortiOS 7.0 系	7.0.0 ～ 7.0.13	7.0.14 以降	2024/2/9 リリース済

(＊1) 6.x 系のバージョンには影響ありません。

3. 回避策

各インターフェースにおいて、fgfm へのアクセス許可を削除することにより回避可能です。これにより、FortiManager から FortiGate の検出が出来なくなりますが、FortiGate からの接続は引き続き可能です。

なお、local-in policy により、FGFM アクセスを特定の IP アドレスに制限することは、特定の IP アドレスに対する脆弱性は残るため、軽減策としては利用できますが、回避策とはなりません。

portX の fgfm へのアクセス許可を制限する例を以下に示します。

```
＜変更前＞
config system interface
    edit "portX"
        set allowaccess ping https ssh fgfm
    next
end

＜変更後＞
config system interface
    edit "portX"
        set allowaccess ping https ssh
    next
end
```

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