2024 年 3 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 のキャプティブポータルにおける境界外書き込みの脆弱性 (CVE-2023-42789, CVE-2023-42790)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 のキャプティブポータル(captive portal)における境界外書き込みの脆弱性(CVE-2023-42789, CVE-2023-42790)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。

敬具

記

1. 事象の概要

FortiOS のキャプティブポータルにおいて、境界外書き込み及びスタックベースのバッファオーバーフローに関する脆弱性があり、悪意のある攻撃者がリモートからキャプティブポータル経由で細工された HTTP リクエストを介して、任意のコードやコマンドを実行でき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 & FortiProxy - Out-of-bounds Write in captive portal
<https://fortiguard.fortinet.com/psirt/FG-IR-23-328>

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 ～ 7.4.1	7.4.2 以降	7.4 系は弊社未リリースです
2	FortiOS 7.2 系	7.2.0 ～ 7.2.5	7.2.6 以降	弊社リリース済
3	FortiOS 7.0 系	7.0.0 ～ 7.0.12	7.0.13 以降	弊社リリース済
4	FortiOS 6.4 系	6.4.0 ～ 6.4.14	6.4.15 以降	弊社リリース済
5	FortiOS 6.2 系	6.2.0 ～ 6.2.15	6.2.16 以降	弊社リリース済 6.2 系 OS はメーカーサポート終了済(EOS 済)

(＊1)FG-30E, FG-50E, FWF-50E-2R, FGR-30D, FGR-35D は 6.2 系が最終 OS の為、6.2 系がサポートされます。

3. 回避策

フォーム認証を無効化することにより回避可能です。

“schemeX”における設定方法の例を以下に示します。

（以下の設定において、set method に form を設定している場合に脆弱性の影響を受けます）

```
config authentication scheme
    edit “schemeX”
        set method <method>
    next
end
```

<method>には以下のいずれかが設定可能です。

ntlm	NTLM authentication.
basic	Basic HTTP authentication.
digest	Digest HTTP authentication.
form	Form-based HTTP authentication.
negotiate	Negotiate authentication.
fsso	Fortinet Single Sign-On (FSSO) authentication.
rsso	RADIUS Single Sign-On (RSSO) authentication.
ssh-publickey	Public key based SSH authentication.
cert	Client certificate authentication.
saml	SAML authentication

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