2023 年 7 月 20 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 のプロキシモードと SSL ディープインスペクションに関するスタックバッファオーバーフローの脆弱性(CVE-2023-33308)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 のプロキシモードと SSL ディープインスペクションに関するスタックバッファオーバーフローの脆弱性(CVE-2023-33308)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 において、スタックバッファオーバーフローの脆弱性により、SSL ディープインスペクションと同時に、プロキシポリシーまたはプロキシモードのファイアウォールポリシーを利用している場合、細工されたパケットを介してリモートの攻撃者が任意のコードやコマンドを実行できる可能性のある脆弱性が見つかりました。

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 - Proxy mode with deep inspection - Stack-based buffer overflow
<https://fortiguard.fortinet.com/psirt/FG-IR-23-183>

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。
なお、FortiOS 6.4 系/6.2 系/6.0 系については、本脆弱性の影響を受けません。

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 ～ 7.2.3	7.2.4 以降	
2	FortiOS 7.0 系	7.0.0 ～ 7.0.10	7.0.11 以降	

3. 回避策

プロキシポリシーまたはプロキシモードのファイアウォールポリシーで利用している SSL インスペクションプロファイルで、HTTP/2 を無効にすることにより回避可能です。以下に設定例を示します。

```
config firewall ssl-ssh-profile
  edit ＜インスペクションプロファイル名>
    set supported-alpn http1-1
  next
end
```

詳細は以下の Fortinet 社のドキュメントを参照してください。

HTTP/2 support in proxy mode SSL inspection
<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl-inspection>

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