

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 SSL-VPN に関するヒープバッファオーバーフローの脆弱性(FG-IR-23-097)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 SSL-VPN に関するヒープバッファオーバーフローの脆弱性(FG-IR-23-097)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 において、SSL-VPN に関するヒープバッファオーバーフローの脆弱性により、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 - Heap buffer overflow in sslvpn pre-authentication

<<https://fortiguard.fortinet.com/psirt/FG-IR-23-097>>

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 ~ 7.2.4	7.2.5(※1)以降	
2	FortiOS 7.0 系	7.0.0 ~ 7.0.11	7.0.12(※1)以降	
3	FortiOS 6.4 系	6.4.0 ~ 6.4.12	6.4.13(※1)以降	
4	FortiOS 6.2 系	6.2.0 ~ 6.2.13	6.2.14以降	
5	FortiOS 6.0 系	6.0.0 ~ 6.0.16	6.0.17(※1)以降	6.0 系 OS はメーカーサポート終了済(EOS 済み)
6	FortiOS(6000 シリーズ) 7.0 系	7.0.5, 7.0.10	7.0.12 以降	
7	FortiOS(6000 シリーズ) 6.4 系	6.4.2, 6.4.6, 6.4.8, 6.4.10, 6.4.12	6.4.13 以降	
8	FortiOS(6000 シリーズ) 6.2 系	6.2.4, 6.2.6, 6.2.7, 6.2.9 ~ 6.2.13	6.2.15 以降(予定)	

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
9	FortiOS(6000 シリーズ) 6.0 系	6.0.10, 6.0.12 ~ 6.0.16	6.0.17 以降 (予定)	6000 シリーズの 6.0 系 OS は弊社未リリース

※1 2023/6/14(水)に弊社からのリリース済です。

3. 回避策

SSL-VPN を無効にすることにより回避可能です。SSL-VPN の無効化の方法については、以下の Fortinet 社の Technical Tip を参照してください。

なお、対策バージョンでは本脆弱性以外の脆弱性の修正も行われているため、Fortinet 社からは対策バージョンにバージョンアップすることが強く推奨されています。

Technical Tip: How to disable SSL VPN functionality on FortiGate

<<https://community.fortinet.com/t5/FortiGate/Technical-Tip-nbsp-How-to-disable-SSL-VPN-functionality-on/ta-p/230801>>

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 ファイルをご入用の場合は、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