2022 年 12 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 SSL-VPN に関するヒープ・オーバーフローの脆弱性(CVE-2022-42475)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・オーバーフローの脆弱性(CVE-2022-42475)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・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。

Fortinet 社からは、既にこの脆弱性を悪用した攻撃が確認されていること、および緊急での対処が必要である旨が、アナウンスされています。

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。

FortiOS - heap-based buffer overflow in sslvpnd
<https://fortiguard.fortinet.com/psirt/FG-IR-22-398>

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<br>バージョン | 対策<br>バージョン | 備考 |
|---|---|---|---|---|
| 1 | FortiOS 7.2 系 | 7.2.0 ～ 7.2.2 | 7.2.3 以降 | 7.2 系 OS は弊社未リリース |
| 2 | FortiOS 7.0 系 | 7.0.0 ～ 7.0.8 | 7.0.9 以降 | |
| 3 | FortiOS 6.4 系 | 6.4.0 ～ 6.4.10 | 6.4.11 以降 | |
| 4 | FortiOS 6.2 系 | 6.2.0 ～ 6.2.11 | 6.2.12 以降 | |
| 5 | FortiOS(6000 シリーズ) 7.0 系 | 7.0.0 ～ 7.0.7 | 7.0.8 以降 | 6000 シリーズの 7.0 系 OS は弊社未リリース |
| 6 | FortiOS(6000 シリーズ) 6.4 系 | 6.4.0 ～ 6.4.9 | 6.4.10 以降 | |
| 7 | FortiOS(6000 シリーズ) 6.2 系 | 6.2.0 ～ 6.2.11 | 6.2.12 以降 | |
| 8 | FortiOS(6000 シリーズ) 6.0 系 | 6.0.0 ～ 6.0.14 | 6.0.15 以降 | 6000 シリーズの 6.0 系 OS は弊社未リリース |

3. 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。

4. 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