2022 年 12 月 22 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 (第四報)

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 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。

※太字箇所が、第四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、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。なお、SSL-VPN をご利用いただいていない場合、本脆弱性の影響を受けません。

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 ～ 7.2.2	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 6.0 系	6.0.0 ～ 6.0.15	6.0.16(※1) 以降	6.0 系 OS はメーカーサポート終了済(EOS 済み)
6	FortiOS 5.6 系	5.6.0 ～ 5.6.14	現時点で なし	5.6 系 OS はメーカーサポート終了済(EOS 済み)

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
7	FortiOS 5.4 系	5.4.0 ～ 5.4.13	現時点で なし	5.4 系 OS はメーカーサポート終了済(EOS 済み)
8	FortiOS 5.2 系	5.2.0 ～ 5.2.15	現時点で なし	5.2 系 OS はメーカーサポート終了済(EOS 済み)
9	FortiOS 5.0 系	5.0.0 ～ 5.0.14	現時点で なし	5.0 系 OS はメーカーサポート終了済(EOS 済み)
10	FortiOS(6000 シリーズ) 7.0 系	7.0.0 ～ 7.0.7	7.0.8 以降 (予定)	6000 シリーズの 7.0 系 OS は弊社未リリース
11	FortiOS(6000 シリーズ) 6.4 系	6.4.0 ～ 6.4.9	6.4.10**(※2)** 以降	
12	FortiOS(6000 シリーズ) 6.2 系	6.2.0 ～ 6.2.11	6.2.12 以降 (予定)	
13	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

※1 2022 年 12 月 16 日に弊社からリリース済です。

※2 2022 年 12 月 19 日に弊社からリリース済です。

3. 回避策

SSL-VPN をご利用の場合、SSL-VPN を無効にすることにより回避可能です。無効化の方法については、「別紙 SSL-VPN の無効化方法」を参照してください。

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. IPS シグネチャでの対応状況

本脆弱性に対応した IPS シグネチャ[1]が IPS パッケージ version 22.430 以降で、リリースされています。シグネチャによる誤検知防止の観点から、当該シグネチャの新規リリース(version 22.430)時点では、検知時の既定のアクションは通信を許可する設定となっています。2022 年 12 月 14 日リリースの version 22.457 で、検知時のデフォルトのアクションは Block に変更されています。このため、version 22.457 未満で通信を制限するには、検知時のアクションを Block にするなどの設定が必要です。

尚、IPS によりブロック可能な通信は、該当の FortiGate を通過する通信となります。IPS では FortiGate 自身に対する通信をブロックできないため、FortiGate 自身の対策にはならないことにご注意ください。

[1] FortiOS.SSL-VPN.Heap.Buffer.Overflow
https://www.fortiguard.com/encyclopedia/ips/52258

6. 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。

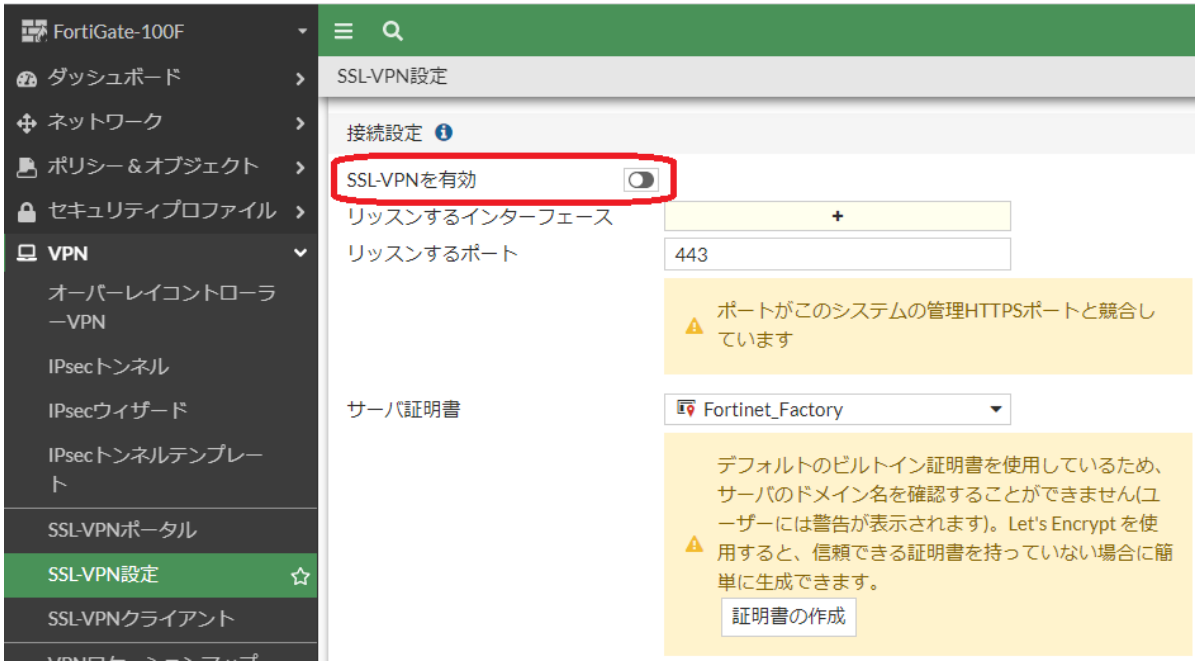
FortiGuard Labs PSIRT Advisories
<https://www.fortiguard.com/psirt>

FortiGuard Labs RSS Feeds
<https://www.fortiguard.com/rss-feeds>

以上

別紙 SSL-VPN の無効化方法
SSL-VPN の無効化方法は、ご利用のバージョンにより異なります。

■ご利用のバージョンが 7.2 系、7.0 系または 6.4.9 以降の場合
＜GUI で設定する場合＞
WebUI で VPN -> SSL-VPN 設定を表示して、「SSL-VPN を有効」をオフにしてください。



＜CLI で設定する場合＞
VDOM の利用有無で設定方法が異なります。

VDOM を利用していない場合：

```
# config vpn ssl settings
    set status disable
    end
```

VDOM を利用している場合：

```
# config vdom
    edit <vdom name>
        config vpn ssl settings
            set status disable
    end
```

■ご利用のバージョンが 6.4.8 以前、6.2 系、6.0.系の場合
VDOM の利用有無で設定方法が異なります。

VDOM を利用していない場合：

```
# config system interface
    edit ssl.root
        set status down
end
```

VDOM を利用している場合：

```
# config vdom
    edit <vdom name>
        config system interface
            edit ssl.root
                set status down
end
```

以上