2019 年 9 月 12 日

株式会社ネットワールド

# CVE-2018-13379　FortiGate　SSL-VPN 脆弱性について

このたびFortinet社が提供するFortiGate製品にて以下脆弱性があることがわかりましたので、以下の通りご報告させて頂きます。

1. 対象製品について

   SSL VPN サービス（Web モードまたはトンネルモード）が有効になっている全ての FortiGate

   【対象 OS】

   FortiOS v6.0.0 から v6.0.4

   FortiOS v5.6.3 から v5.6.7

   FortiOS v5.4.6 から v5.4.12

2. 概要について

   FortiOS SSL VPN Web ポータルのパストラバーサルの脆弱性により、認証されていない攻撃者が特別に細工された HTTP リソースリクエストを介して FortiOS システムファイルをダウンロードする可能性があります。

3. 対策について

   本脆弱性を回避する方法は以下の通りです。

   FortiOS v5.6.8以上へのアップグレード

   FortiOS v6.0.5以上へのアップグレード

   FortiOS v6.2.0以上へのアップグレード

   ※v6.2のサポートは行ってはおりませんが、ご要望があればファームウェアの提供は可能です。※サポート開始は今現在未定になります。

4. 一時的なワークアラウンドについて

   以下 CLI コマンドより、SSL-VPN サービス（Web モードとトンネルモードの両方）を無効にしてください。

```
config vpn ssl settings
unset source-interface
end
```

上記設定を行うには、SSL VPN に関連付けられたファイアウォールポリシーを最初に削除する必要があります。

たとえば、source-interface が「port1」で、SSL VPN インターフェースが「ssl.root」の場合、「unset source-interface」の前に、次の CLI コマンドが必要です。

```
config vpn ssl settings
config authentication-rule
purge（すべてのルールを削除します。）
end
end

config firewall policy
delete [policy-id]（srcintf が「ssl.root」で dstintf が「port1」である SSL VPN ポリシーID）
end
```

・メーカ提供情報

URL：

https://fortiguard.com/psirt/FG-IR-18-384

・参考情報（JPCERT）

URL：

https://www.jpcert.or.jp/at/2019/at190033.html

以上