2020 年 12 月 4 日

お客様各位

株式会社日立ソリューションズ
Fortinet 製品ユーザーサポート

SSL-VPN 機能の脆弱性(CVE-2018-13379)の影響を受けるホスト情報の公開について

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。

一部のニュースサイトで、FortiOS の SSL-VPN 機能の脆弱性(CVE-2018-13379)の対策がされていない IP アドレス一覧(日本企業含む)が一部フォーラム等で公開された旨の報道がされています。SSL-VPN 機能をご利用で、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、若しくは SSL-VPN 機能の停止のご検討をお願いいたします。

敬具

記

１．概要

2019 年 5 月に開示されている FortiOS の SSL-VPN 機能の脆弱性(CVE-2018-13379 (*1))の対策がされていない機器の IP アドレス一覧(日本企業含む)が一部フォーラム等で公開された旨の報道がされています。

この脆弱性では、攻撃者に FortiGate/FortiWiFi 機器内部のファイルを参照される可能性があります。認証情報等が参照/漏洩した場合、この認証情報が用いられ、組織ネットワークへのさらなる攻撃が行われる可能性があります。

その為、脆弱性の影響を受けるバージョンで SSL-VPN 機能を利用されている場合は、バージョンアップ若しくは、SSL-VPN 機能の停止のご検討をお願いします。

２．影響を受けるバージョン

メジャーバージョンごとの影響を受けるバージョンは以下の通りです。

6.2 系の OS は本脆弱性の影響は受けません。

項	メジャーバージョン	影響を受けるバージョン
1	FortiOS 6.0 系	6.0.0 から 6.0.4 迄のバージョン
2	FortiOS 5.6 系	5.6.3 から 5.6.7 迄のバージョン
3	FortiOS 5.4 系	5.4.6 から 5.4.12 迄のバージョン

３．対策

緩和策として 2 要素認証の利用が提示されていますが、根本対策はバージョンアップのみです。

本脆弱性が対策されているバージョンは以下の通りです。

尚、5.4 系は既に Fortinet 社のサポートが終了。また、5.6 系も開発が終了しております。他、SSL-VPN 機能は今回以外にも脆弱性が報告されています(*2)。その為、6.0 系又は 6.2 系の最新バージョンへのバージョンアップを合わせてご検討下さい。

バージョンアップで必要となる OS ファイル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下さい。

項	メジャーバージョン	対策バージョン	備考
1	FortiOS 6.2 系	6.2.0 以降	6.2.6 までリリース済み
2	FortiOS 6.0 系	6.0.5 以降	6.0.11 までリリース済み 2021/03/29 で EOES
3	FortiOS 5.6 系	5.6.8 以降	5.6.13 までリリース済み 2021/09/30 で EOS
4	FortiOS 5.4 系	5.4.13	2020/06/21 で EOS

※EOES(End of Engineering Support)：Fortinet 社開発での調査終了。以後は、Fortinet 社の調査やトラブルシューティングは限定されます。以後は一部の脆弱性対策等を除き、不具合対策 OS 等のリリースはされません。
EOS (End of Support)：Fortinet 社サポート終了。以後は弊社のノウハウを元にサポートを実施します。回避策を中心に情報提供を行います。
詳しくは、弊社サポートサイト End Of Support 項を参照下さい。
https://csps.hitachi-solutions.co.jp/fortinet/end_of_support.html

---

(*1)Fortinet 社では、脆弱性情報は FortiGuard Labs の PSIRT Advisory で公開しています。CVE-2018-13379 に該当するアドバイザリは以下の通りです。
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。

FortiOS system file leak through SSL VPN via specially crafted HTTP resource requests
https://www.fortiguard.com/psirt/FG-IR-18-384

(*2)2019 年以降では、SSL-VPN の脆弱性として以下のアドバイザリが公開されています。

FortiOS multiple pre-auth XSS vulnerabilities on SSL VPN
https://www.fortiguard.com/psirt/FG-IR-18-383

FortiOS SSL VPN buffer overrun through POST message payload
https://www.fortiguard.com/psirt/FG-IR-18-387

SSL VPN buffer overrun when parsing javascript href content
https://www.fortiguard.com/psirt/FG-IR-18-388

Unauthenticated SSL VPN users password modification
https://www.fortiguard.com/psirt/FG-IR-18-389

FortiOS SSL VPN web portal Host Header Redirection
https://www.fortiguard.com/psirt/FG-IR-19-002

FortiOS reflected XSS in the SSL VPN web portal error page parameters
https://www.fortiguard.com/psirt/FG-IR-19-034

FortiOS SSL VPN user credential plaintext storage
https://www.fortiguard.com/psirt/FG-IR-19-217

FortiOS SSL VPN 2FA bypass by changing username case
https://www.fortiguard.com/psirt/FG-IR-19-283

以上