2021 年 4 月 8 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

米国政府機関による FortiOS の脆弱性をついた攻撃への注意喚起について

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。

米国政府機関（FBI 及び CISA）から、標的型攻撃の攻撃者が FortiOS の既知の脆弱性を持つ機器を調査、悪用しようとしている旨、注意喚起が行われています。

今回の脆弱性は新たなものではなく、これまでに公開済みの脆弱性(2019 年 5 月から 2020 年 7 月)ではありますが、お客様におかれましては、今一度影響有無をご確認頂きますようお願い致します。また、これら脆弱性の影響を受けるバージョンをご利用のお客様は、改めて対策済み OS へのバージョンアップの実施をお願いいたします。

敬具

記

1　概要

2021 年 4 月 2 日に、FBI(米連邦捜査局)及び CISA(米サイバーセキュリティインフラストラクチャセキュリティ庁)が共同で、2021 年 3 月に標的型攻撃(ATP)を行う攻撃者が FortiOS の既知の脆弱性(CVE-2018-13379, CVE-2020-12812, CVE-2019-5591)を持つ機器を調査、悪用しようとしている旨、注意喚起(*1)が行われています。

脆弱性の影響を受けるバージョンを利用されている場合は、組織のネットワークへの侵入等、攻撃に利用される可能性があります。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の実施をお願いいたします。

2　脆弱性概要

注意喚起された脆弱性の概要は以下の通りです。

詳細については、Fortinet 社から個々に発表されています PSIRT Advisories(*2)をご覧下さい。

2.1　CVE-2018-13379 (Fortinet 社アドバイザリ番号：FG-IR-18-384 (*3))

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にシステムファイルをダウンロードされる可能性があります。

この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。尚、6.2 系及び 6.4 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	対策バージョン
1	FortiOS 6.0 系	6.0.0 から 6.0.4 迄のバージョン	6.0.5 以降
2	FortiOS 5.6 系	5.6.3 から 5.6.7 迄のバージョン	5.6.8 以降
3	FortiOS 5.4 系	5.4.6 から 5.4.12 迄のバージョン	5.4.13

この脆弱性については、2020 年 12 月 4 日付で当サイトでも案内をしております為、そちらも合わせてご参照下さい。

また、6.0 系までの OS は、既に EOES または EOS を迎えています(*6)。バージョンアップにあたっては、6.2 系または 6.4 系の OS のご検討をお願い致します。

2.2　CVE-2020-12812(Fortinet 社アドバイザリ番号：FG-IR-19-283 (*4))

SSL-VPN の認証の脆弱性により、2 要素認証(FortiToken)を利用しており、また、ユーザ名の大文字と小文字を変更した場合、2 要素目の入力を求められずにログインできる可能性があります。

この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。

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
1	FortiOS 6.4 系	6.4.0	6.4.1 以降
2	FortiOS 6.2 系	6.2.0 から 6.2.3 迄のバージョン	6.2.4 以降
3	FortiOS 6.0 系以下	6.0.9 迄のバージョン	6.0.10 以降

2.3　CVE-2019-5591(Fortinet 社アドバイザリ番号：FG-IR-19-037 (*5))

デフォルト設定で LDAP サーバを利用している場合、同一サブネット上にいる攻撃者が LDAP サーバになりすますことができます。

この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。

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
1	FortiOS 6.2 系以下	6.2.0 迄のバージョン	6.2.1 以降

尚、6.0.3 以降のバージョンの場合は、LDAP 設定で、プロトコルを LDAPS に変更し、”server-identity-check”設定を有効にすることで対策することができます。6.2.1 以降ではこの設定がデフォルトで有効になっています。

また、対策バージョンであっても、バージョンアップを行った場合は、バージョンアップ前のコンフィグを引き継ぐ為、手動で LDAPS の設置と”server-identity-check”設定を有効にする必要があります。

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下さい。

4　定期的な脆弱性情報の確認とバージョンアップのお願い

Fortinet 製品の脆弱性情報は、Fortinet 社 FortiGuard Labs の PSIRT Advisory で公開されています。脆弱性情報につきましては定期的にご参照頂くとともに、ご利用の環境が脆弱性を持つ場合は、必要に応じて設定見直し、また対策済みバージョンへのバージョンアップを実施頂きますようお願い致します。

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記載内容以上の情報については、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。

以上

(*1)出典
FBI-CISA Joint Advisory on Exploitation of Fortinet FortiOS Vulnerabilities
https://us-cert.cisa.gov/ncas/current-activity/2021/04/02/fbi-cisa-joint-advisory-exploitation-fortinet-fortios

APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks
https://www.ic3.gov/Media/News/2021/210402.pdf

(*2)Fortinet 社 FortiGuard Labs PSIRT Advisory
https://www.fortiguard.com/psirt

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

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

(*5)FortiGate default configuration does not verify the LDAP server identity.
https://www.fortiguard.com/psirt/FG-IR-19-037

(*6) 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