事　務　連　絡
令和４年12月16日

各都道府県衛生主管部（局）　御中

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
厚生労働省政策統括官付サイバーセキュリティ担当参事官室

FortiOSに関する脆弱性情報への対応について（注意喚起）

昨今、医療機関において、ランサムウェアによるサイバー攻撃事案が発生し、電子カルテの閲覧・利用ができなくなる等により、地域の医療提供体制に影響が出る事案が複数発生しているところです。これらの事案に共通する攻撃者の侵入経路として、医療機関と外部機関（主にベンダーや取引事業者等）を接続する通信機器とそのソフトウェア（以下「ゲートウェイ装置」という。）の脆弱性を通じて行われていることが指摘されています。

特に、FortiOSについては、本年10月に続き、12月にも脆弱性が発見されておりますので、下記を参考にセプター等を通じて情報提供した「Fortinet製品の深刻な脆弱性について（注意喚起）」（参考１）等へ速やかに対応するよう周知をお願いします。

記

１　ゲートウェイ装置の使用状況の確認

各医療機関のシステムを管理するベンダーに対し、セプター等から提供された脆弱性情報の対象となるソフトウェアが使用されているか、及びサポート期限が切れていないかを確認するよう依頼すること。

２　脆弱性への対応及び緩和策の実施

上記１の確認の結果、対象ソフトウェアを使用している場合には、事前にログ等を保全した上で速やかに最新のソフトウェアにバージョンアップする等の必要な対応を実施すること。

３　侵害の兆候の確認

「Fortinet製品の深刻な脆弱性について（注意喚起）」のように、攻撃を受けた場合に記録されるログ、悪性IPアドレス、ネットワーク機器のファイルシステム上に作成されるファイル名が示されている場合、ログ等を確認し攻撃の兆候がないか確認するこ

と。

なお、自組織内またはベンダーが確認した結果、攻撃の兆候が認められた場合は、医政局特定医薬品開発支援・医療情報担当参事官室もしくは医療機関向けセキュリティ教育支援ポータルサイト上の「インシデントかも？」を通じて報告すること。

※医療機関向けセキュリティ教育支援ポータルサイトはこちら

https://mhlw-training.saj.or.jp/

4　その他

その他令和４年 11 月 10 日付け事務連絡「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」（参考２）等も踏まえ、適確なサイバーセキュリティ対策を講じること。

以上

参考１

TLP:CLEAR【全分野】

別紙

2022年12月14日

内閣官房　内閣サイバーセキュリティセンター
重要インフラグループ

Fortinet製品の深刻な脆弱性について（注意喚起）（第２報）

2022年12月13日（火）（日本時間）、Fortinetはアドバイザリを更新し、本脆弱性の影響を受ける対象バージョンとして、FortiOS 5系及び6.0系を追加しました。また、本脆弱性の回避策として、SSL-VPNの無効化を追加しました。本第２報は第１報（2022年12月13日付けFortinet製品の深刻な脆弱性について（注意喚起））の内容を含むものとなっています。

NISCにおいて、当該製品のようなネットワーク機器の脆弱性を突く攻撃の発生を確認しています。この脆弱性が悪用され、組織内ネットワークが侵害された場合、ランサムウェア等により被害が甚大になる恐れがあるため、即時のバージョンアップを強く推奨します。また、サプライチェーン攻撃等、自組織以外の接続先から侵害を受ける可能性もあるため、この点についても、十分以上に留意してください。

1. 対象ソフトウェア
   - FortiOS　5.0.0から5.0.14、5.2.0から5.2.15、5.4.0から5.4.13、5.6.0から5.6.14、6.0.0から6.0.15、6.2.0から6.2.11、6.4.0から6.4.10、7.0.0から7.0.8、7.2.0から7.2.2
     *ハードウェアサポートが継続している一部製品の場合を除き、5系及び6.0系はサポート対象外のため、直ちにバージョンアップをしてください。
   - FortiOS-6K7K　6.0.0から6.0.14、6.2.0から6.2.11、6.4.0から6.4.9、7.0.0から7.0.7

2. 脆弱性悪用による影響等
   対象ソフトウェアを使用しているネットワーク機器に対して、攻撃者による任意のコード実行等の恐れがあります。

3. 深刻度
   ソフトウェアの開発元が深刻度「Critical」（5段階中、最高）に分類する脆弱性が含まれます。

4. 悪用
   開発元により脆弱性を悪用した攻撃が確認されています。

5. 対応
   対象ソフトウェアを最新のバージョンに更新してください。

加えて、侵害の兆候がないか確認するとともに、監視の強化（本項目参照）等についても検討してください。

開発元が公開している侵害の兆候を以下に示します。

(1) ログ

攻撃を受けた際、次の特徴的なログが記録されます。

Logdesc="Application crashed" and msg="[…] application:sslvpnd,[…], Signal 11 received, Backtrace: […] "

(2) 悪性 IP アドレス

現在のところ、ネットワーク機器から次の疑わしい IP アドレス宛ての通信が確認されています。

188.34.130.40:444
103.131.189.143:30080,30081,30443,20443
192.36.119.61:8443,444
172.247.168.153:8033

(3) ファイル

現在のところ、攻撃を受けた際、対象ソフトウェアを使用しているネットワーク機器のファイルシステム上に次のファイルが作成されます。

/data/lib/libips.bak
/data/lib/libgif.so
/data/lib/libiptcp.so
/data/lib/libipudp.so
/data/lib/libjepg.so
/var/.sslvpnconfigbk
/data/etc/wxd.conf
/flash

6. その他

SSL-VPN を無効化することで本脆弱性の影響を回避できますが、直ちにバージョンアップを行うことを強く推奨します。

参考 URL

- FortiOS – Heap-based buffer overflow in sslvpnd (Fortinet)
  https://www.fortiguard.com/psirt/FG-IR-22-398
- FortiOS のヒープベースのバッファーオーバーフローの脆弱性 (CVE-2022-42475) に関する注意喚起 (JPCERT/CC)
  https://www.jpcert.or.jp/at/2022/at220032.html
- FortiOS SSL-VPN の脆弱性対策について (CVE-2022-42475) (IPA)
  https://www.ipa.go.jp/security/ciadr/vul/alert20221213.html