青い森のサイバーセキュリティ

令和５年８月
青森県警察本部
サイバー犯罪対策課

Fortinet社製品に新たな脆弱性

◎Fortinet製品の別の脆弱性が公開

３月に続き、Fortigateを始めとする複数のFortinet製品に関する脆弱性情報が公開されました。この脆弱性を放置したままにすると、悪意の第三者によって攻撃に悪用され、外部から任意のコード(プログラム)を内部システム上で実行される可能性があります。

該当する機器を使用中の方は早急に対策の実施をお願いします。

◆今回公開された脆弱性情報(CVE－2023－27997)

【影響を受けるシステム／バージョン】

・FortiOS　：7.2.0～7.2.4、7.0.0～7.0.11、6.4.0～6.4.12、6.2.0～6.2.13、6.0.0～6.0.16

・FortiProxy　：7.2.0～7.2.3、7.0.0～7.0.9、2.0.0～2.0.12、1.2系の全て、1.1系の全て

・FortiOS6K7K：7.0.10、7.0.5、6.4.12、6.4.10、6.4.8、6.4.6、6.4.2、6.2.9～6.2.13、6.2.6～6.2.7、6.2.4、6.0.12～6.0.16、6. 0. 10

※赤字部分が3月公開情報との相違点

◎対策

【推奨】

・ それぞれ脆弱性が修正されたバージョンのOSに更新する。

【上記が早急にできない場合のリスク緩和策】

・ SSL-VPNを無効化する。

■ 詳細についてはFortinet社のページを参照してください。
FotiOS / FortiProxy - Heap buffer overflow in sslvpn pre-authentication
https://www.fortiguard.com/psirt/FG-IR-23-097