滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R４年度 No.２３
今、注目のサイバーセキュリティに関する情報をお届けします。

「FortiOS」の脆弱性に関する注意喚起情報

IPS(不正侵入防止システム)やVPN(仮想専用通信網)、ファイアウォール機器などを提供しているFortinet社から、同社の製品で使用されている「FortiOS」に関する脆弱性情報(CVE-2022-42475、CVSSスコア9.3(緊急))が発表されています。今回の情報提供は技術的な内容を含みますので、自組織のシステム担当者やシステム委託業者に確認していただき、同社製の機器を利用されていて今回の脆弱性情報に該当される場合は対応を御検討ください。

脆弱性の概要

今回発表された「FortiOS」の脆弱性は、「FortiOS SSL-VPN」のヒープベース(メモリ領域)のバッファオーバーフロー(大きなデータ量を入力してオーバーフローを起こし、メモリ領域を書き換える攻撃手法)の脆弱性です。

この脆弱性が悪用されると、攻撃者が認証を回避して、遠隔で任意のコードやコマンドを実行することができるようになり、各種システムへの侵入や乗っ取りが可能となります。

12月13日現在、PoC(脆弱性の検証コード)情報の公開は確認されていませんが、Fortinet社は、この脆弱性を悪用した攻撃を確認したとしています。

対　策

Fortinet社では、影響受ける「FortiOS」のバージョンについて、該当バージョンの「FortiOS」を使用している場合は、アップグレードを推奨しています。

製品名	影響を受けるバージョン	修正後バージョン
FortiOS	7.2.0から7.2.2	7.2.3以降
FortiOS	7.0.0から7.0.8	7.0.9以降
FortiOS	6.4.0から6.4.10	6.4.11以降
FortiOS	6.2.0から6.2.11	6.2.12以降
FortiOS-6K7K	7.0.0から7.0.7	7.0.8以降
FortiOS-6K7K	6.4.0から6.4.9	6.4.10以降
FortiOS-6K7K	6.2.0から6.2.11	6.2.12以降
FortiOS-6K7K	6.0.0から6.0.14	6.0.15以降

攻撃の有無の確認

攻撃の有無を確認するためのログやIPアドレスなどの情報については、Fortinet社が公開しています。以下のＵＲＬから御確認ください。

【Fortinet社】https://www.fortiguard.com/psirt/FG-IR-22-398
【参考：JPCERT注意喚起情報】https://www.jpcert.or.jp/at/2022/at220032.html

Fortinet社製品は、外部から内部システムへ入るときの入口部分にあたる機器に多く利用されており、一度、この機器のセキュリティが突破されてしまうと、内部システムへの影響が甚大となります。是非とも、この注意喚起情報をシステム担当者等と共有していただき、万が一、被害が発生したり、前兆事案を把握された場合は、警察にも御一報ください。