滋賀県警察サイバーセキュリティ情報
R５年度 No. 8
サイバーコネクトSHIG@
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」及び「FortiProxy」に関する脆弱性情報(CVE-2023-33308、CVSSスコア9.8(重要度:緊急))が発表されています。今回の脆弱性情報は深刻度が高いことから、自組織のシステム担当者やシステム委託業者に速やか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

発表された脆弱性は、「FortiOS」及び「FortiProxy」のスタックベース(メモリ領域)のバッファオーバーフロー(サーバ等に処理能力を超える大量のデータや悪意のあるコードを送って実行中のプログラムを強制停止したり、管理者権限を取得したりする攻撃手法)の脆弱性です。

この脆弱性は、「FortiOS」等でSSLディープインスペクション(SSLで暗号化されている通信が制御装置を通過するときに、一旦通信データを復号し、内容を確認した後に再暗号化する機能)をプロキシモードで使用している時、プロキシポリシー又はファイアウォールポリシーに細工したパケットを到達させることで、悪意のあるコードやコマンドが実行される可能性があるものです。

影響を受けるバージョン

影響を受ける「FortiOS」等のバージョンは次のとおりです。

FortiOS	7.2.0～7.2.3、7.0.0～7.0.10
Forti Proxy	7.2.0～7.2.2、7.0.0～7.0.9

なお、「FortiOS」バージョン6.4系、6.2系、6.0系、「Forti Proxy」バージョン2.x系、1.x系のすべてのバージョンは、今回の脆弱性の影響を受けないとされています。

影響を受けるバージョンを利用されている場合は、対策済みのOSにバージョンアップをお願いします。最新の情報については、Fortinet社のWebページを参照してください。

【Fortinet社】https://www.fortiguard.com/psirt/FG-IR-23-183

回避策

次の対処方法が紹介されていますが、あくまでも暫定のものとして、メーカーでは「FortiOS」等のバージョンアップを推奨しています。

【回避策１】ディープインスペクション機能を無効にする。ただし、通信制御に支障が生じるおそれがある。

【回避策２】プロキシポリシー又はプロキシモードのファイアウォールポリシーによって使用されるSSL検査プロファイルでのHTTP/2サポートを無効にする。無効にするワークアラウンド(応急措置のコマンドライン)がFortinet社から提供されているので、前述のFortinet社のWebページを参照してください。

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。