2025 年 1 月 17 日

お客様各位

株式会社日立ソリューションズ
Fortinet 製品ユーザサポート

【脆弱性】FortiOS 7.0 系における認証バイパスの脆弱性(CVE-2024-55591)について(第二報)

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。

この度 Fortinet 社より、深刻度の高い脆弱性として、FortiOS の Node.js における認証バイパスの脆弱性(CVE-2024-55591)がアナウンスされています。本脆弱性の影響を受けるバージョンをご利用のお客様におかれましては、対策済み OS へのバージョンアップや回避策の適用について、ご検討をお願いいたします。

※太字箇所が、第二報での追記もしくは更新箇所となっています。

敬具

記

1. 事象の概要

FortiOS における認証バイパスの脆弱性[CWE-288]により、悪意のある攻撃者がリモートから特別に細工された HTTP リクエスト(Node.js websocket module)を経由して、super-admin 権限を取得できる可能性があります。

Fortinet 社は、本脆弱性を悪用した攻撃が起きている可能性があることをアナウンスしています。

詳細、最新の情報については Fortinet 社から発表されています、以下セキュリティアドバイザリ(PSIRT Advisories)をご覧ください。

Authentication bypass in Node.js websocket module
<https://www.fortiguard.com/psirt/FG-IR-24-535 >

2. 該当製品と対策バージョン

弊社取り扱い済みの製品・バージョンにて、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	備考
1	FortiOS 7.4 系	なし	—	
2	FortiOS 7.2 系	なし	—	
3	FortiOS 7.0 系	7.0.16 以前	7.0.17 以降	**弊社からは 1/17(金)にリリース済**
4	FortiOS 6.4 系	なし	—	EOS 済みバージョン

3. 回避策

脆弱性の回避策は以下の通りです。なお、回避策 2 によりアクセス元の IP アドレスを制限した後も、該当 IP アドレスからのアクセスには脆弱性が残るため、早急に対策バージョンへのアップグレードの検討をお願いいたします。

回避策 1

インターフェースにおける HTTP/HTTPS の管理アクセスを無効に設定することにより、本脆弱性の回避が可能です。

回避策 2

local-in-policy により、FortiGate の管理インターフェース(GUI)へのアクセス元の IP アドレスを制限することで、制限した IP アドレス以外からの脆弱性を回避可能です。
local-in-policy による管理インターフェースへのアクセス制限の設定方法については、セキュリティアドバイザリを参照してください。

4. 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ください。

5. Fortinet 社セキュリティアドバイザリ

Fortinet 社では、脆弱性情報を以下、FortiGuard Labs PSIRT Advisories で公開しています。最新の脆弱性情報は以下サイトをご覧頂き、適時ご利用環境の対策をいただきますようお願いします。

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内容等については、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。

PSIRT Advisories は RSS 配信も行われていますので、合わせてご活用ください。

FortiGuard Labs PSIRT Advisories
<https://www.fortiguard.com/psirt>

FortiGuard Labs RSS Feeds
<https://www.fortiguard.com/rss-feeds>

以上