2026 年 5 月 22 日

お客様各位

株式会社日立ソリューションズ
Fortinet 製品ユーザーサポート

【脆弱性】FortiClient EMS における API 認証・認可バイパスの脆弱性 (CVE-2026-35616)について

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、FortiClient EMS における API 認証・認可バイパスの脆弱性(CVE-2026-35616)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で FortiClient EMS をご利用のお客様におかれましては、対策済み OS へのアップグレードもしくは hotfix の適用をご検討いただきますようお願いいたします。

敬具

記

1. 事象の概要

FortiClient EMS における不適切なアクセス制御の脆弱性[CWE-284]により、認証されていない攻撃者が細工されたリクエストを通じて、不正なコードやコマンドを実行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既に起きてい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。

API authentication and authorization bypass
<https://fortiguard.fortinet.com/psirt/FG-IR-26-099 >

2. 該当製品と対策バージョン

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。
影響を受けるバージョンをご利用中の場合は、対策済み OS へのアップグレードをお願いいたします。

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
1	FortiClient EMS 7.4 系	7.4.5～7.4.6	7.4.7 以降
2	FortiClient EMS 7.2 系	影響なし	－

尚、FortiClient EMS にはアップグレードに関する不具合が報告されています。
詳細は以下ページをご覧ください。

FortiClient EMS のアップグレード失敗に伴うデータの損失について(CSB-260410-1)
<https://csps.hitachi-solutions.co.jp/fortinet/data/info_20260522-2.pdf>

直ちに対策バージョンへのアップグレードが難しい場合は、以下のリリースノートを参考に hotfix を適用していただきますようお願いいたします。

Installing an EMS hotfix | FortiClient 7.4.5
<https://docs.fortinet.com/document/forticlient/7.4.5/ems-release-notes/832484>

Installing an EMS hotfix | FortiClient 7.4.6
<https://docs.fortinet.com/document/forticlient/7.4.6/ems-release-notes/832484>

3. 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