2026 年 04 月 06 日
株式会社ネットワールド

FortiClient EMS API の認証および認可のバイパスについて

Fortinet 社の PSIRT(Product Security Incident Response Team)より Critical として、
以下の情報が公開されましたので、以下の通りご報告させていただきます。

概要：
FortiClient EMS のアクセス制御に関する脆弱性［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介し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。

CVE ID：
CVE-2026-35616

影響：
認証なしでアクセスできてしまう問題

バージョン	対象バージョン	対策バージョン
FortiClient EMS v7.4	v7.4.5 ～ v7.4.6	v7.4.7以降へのアップグレードしてください
FortiClient EMS v7.2	影響なし	該当しません

Fortinet は、この脆弱性が実際に悪用されていることを確認しており、影響を受けるお客様に対し、FortiClient EMS7.4.5 および 7.4.6 用のホットフィックスを以下の手順に従ってインストールするよう強く推奨します。

https://docs.fortinet.com/document/forticlient/7.4.5/ems-release-notes/832484 - FortiClientEMS 7.4.5 用
https://docs.fortinet.com/document/forticlient/7.4.6/ems-release-notes/832484 - FortiClientEMS 7.4.6 用

※弊社サーバーの該当バージョンのフォルダへ「**【hotfix】CVE-2026-35616**」を準備しました。こちらより**hotfix**を入手ください。

近日リリース予定の FortiClientEMS 7.4.7 にも、この問題に対する修正が含まれる予定です。それまでの間は、上記のホットフィックスを適用することで、この問題を回避できます。

詳細は以下をご参照ください。
https://fortiguard.fortinet.com/psirt/FG-IR-26-099

以上