

FortiWeb GUI におけるパス混乱の脆弱性について

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：

FortiWeb の相対パス トラバーサル脆弱性 [CWE-23] により、認証されていない攻撃者が細工したHTTP または HTTPS リクエストを介してシステム上で管理コマンドを実行できる可能性があります。

フォーティネットは、これが実際に悪用されているのを確認しております。

CVE ID：

CVE-2025-64446

影響：

不適切なアクセス制御

影響を受けるバージョン：

FortiWeb v8.0 8.0.0 ～ 8.0.1

FortiWeb v7.6 7.6.0 ～ 7.6.3

FortiWeb v7.4 7.4.0 ～ 7.4.9

FortiWeb v7.2 7.2.0 ～ 7.2.11

FortiWeb V7.0 7.0.0 ～ 7.0.11

対策：

FortiWeb 8.0 8.0.2 以上にアップグレードしてください。

FortiWeb 7.6 7.6.5 またはそれ以上にアップグレードしてください。

FortiWeb 7.4 7.4.10 またはそれ以上にアップグレードしてください。

FortiWeb 7.2 7.2.12 またはそれ以上にアップグレードしてください。

FortiWeb 7.0 7.0.12 またはそれ以上にアップグレードしてください。

回避策：

インターネットに接続されたインターフェースで、HTTPまたはHTTPSを無効にしてください。
フォーティネットは、アップグレードが実行可能になるまでこの対策を推奨しています。

ベストプラクティスに従って、HTTP/HTTPS管理インターフェースが内部からのみアクセス可能であれば、リスクは大幅に軽減されます。

アップグレード後の手順：

お客様には、設定を確認し、ログで予期しない変更や不正な管理者アカウントの追加がないか確認することをお勧めします。

詳細は以下をご参照ください。

<https://fortiguard.fortinet.com/psirt/FG-IR-25-910>

以上