

FortiSandbox GUI における不適切なアクセス制御およびセッション管理の脆弱性について

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：

FortiSandbox GUI の代替パスまたはチャンネルを使用した認証バイパスの脆弱性 [CWE-288] により、リモートの認証されていない攻撃者が細工された HTTP リクエストを介して認証をバイパスできる可能性があります。

CVE ID：

CVE-2026-107656

影響：

許可されていないコードまたはコマンドを実行する

影響を受けるバージョンと対策バージョン：

バージョン	影響のあるバージョン	対策バージョン
FortiSandbox 5.2	影響なし	—
FortiSandbox 5.0	v5.0.0 から v5.0.6 まで	v5.0.7 以上にアップグレードしてください
FortiSandbox 4.4	v4.4.0 から v4.4.9 まで	v4.4.10 以上へのアップグレードしてください
FortiSandbox PaaS 5.2	影響なし	—
FortiSandbox PaaS 5.0	v5.0.0 から v5.0.6 まで	v5.0.7 以上にアップグレードしてください
FortiSandbox PaaS 4.4	v4.4 全てのバージョン	v5.0.7 以上にアップグレードしてください

詳細は以下をご参照ください。

<https://fortiguard.fortinet.com/psirt/FG-IR-26-185>

以上