2026 年 6 月 23 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

FortiGate を標的としたサイバー攻撃(FortiBleed)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。

FortiGate において、過去の認証情報を利用したサイバー攻撃(FortiBleed)が確認されております。本件について、Fortinet 社より下記の通りアナウンスされております。

敬具

記

1. 問題の概要

FortiGate において、過去の認証情報を利用したサイバー攻撃(FortiBleed)が確認されております。過去に発生したインシデントに起因する情報が再利用され、製品がブルートフォース攻撃等のサイバー攻撃を受ける可能性があるという問題であり、新規の脆弱性に対する攻撃ではありません。

定期的な認証情報のローテーションや、多要素認証(MFA)の有効化、管理インターフェースをインターネットに交換しない運用といったセキュリティ対策を実施されているお客様におかれましては、認証情報の侵害リスクは最小限と考えられます。

詳細、最新の情報については 以下の Fortinet 社のブログをご参照ください。

Analysis of Reported Credential Compromise of FortiGate Devices
https://www.fortinet.com/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices

【日本語抄訳版】FortiGate デバイスの認証情報を使った攻撃キャンペーンの分析
https://www.fortinet.com/jp/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices

2. 本問題への対応

上記ブログの通り、Fortinet 社は本問題に対し、下記の対応を行うことを推奨しています。

・すべての管理セッション、VPN セッションをリセットし、認証情報をリセット
・すべての管理者アカウント、VPN ユーザアカウントに MFA を設定
・最新バージョンへのアップグレード
・不正な設定変更の有無の検証
・ログのチェック(予期しない IP からの管理アクセス、大量の Login 失敗など)
・管理インターフェースへのアクセスの制限

以上