

2017年 12月28日

お客様各位

株式会社日立ソリューションズ  
Palo Alto Networks 製品ユーザサポート

PAN-OS の Web 管理画面における脆弱性 (CVE-2017-15944) について

拝啓 平素は Palo Alto Networks 製品ユーザサポートをご利用くださいますこと誠にありがとうございます。

この度、PAN-OS にリモートから任意のコードを実行可能な脆弱性が発見されました。本脆弱性は Web 管理画面で認証を行うことなく第三者がコードを実行できるものです。2017年12月21日時点で脆弱性を悪用する攻撃は確認されておりませんが、早期の対策が推奨されるものです。2017年12月14日にメーカより修正版がリリースされております。

※Panorama は本脆弱性を含まないため対象外となっております。

以下、各対象バージョンと対応策を示します。

■脆弱性が含まれるバージョン

- ・ PAN-OS 6.1.18 以前のバージョン
- ・ PAN-OS 7.0.18 以前のバージョン
- ・ PAN-OS 7.1.13 以前のバージョン
- ・ PAN-OS 8.0.5 以前のバージョン

■修正が行われたバージョン

- ・ PAN-OS 6.1.19 以降のバージョン
- ・ PAN-OS 7.0.19 以降のバージョン
- ・ PAN-OS 7.1.14 以降のバージョン
- ・ PAN-OS 8.0.6 以降のバージョン

■対応策

早急な修正版へのバージョンアップをご検討ください。

早期対応が難しい場合は、一時的な回避策として以下をご検討ください。

ただし、あくまで暫定対策となり脆弱性は残ったままとなります。

- コンテンツバージョン **756** 以降を適用する。  
(SSL 復号機能を有効にする必要がございます)
- Panorama を使用したリモート接続のみに制限する。(MGT ポートのサービス設定にて **https**、**http** は無効とする)
- 管理画面へアクセスできる IP アドレスを制限する。

以上