２０１８年　1月１９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（第３報）

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して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。
PA シリーズおよび Panorama(※)をご利用のお客様におかれましては、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 も本脆弱性の対象であることが判明致しました。

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

■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**(※)**
※PAN-OS 8.0.6 以降のバージョンにて本脆弱性の修正が行われておりますが、PAN-OS 8.0 系は、本脆弱性を用いた認証されていないユーザによるリモートアクセスが不可となるため、現状のままでも本脆弱性の影響はございません。

■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）
・管理画面へアクセスできる IP アドレスを制限する。
・インターネットを介した Web 管理インターフェイスへの接続は VPN 接続を使用する。

※不必要なインターネットへの Web 管理ポートの公開はお控えください。

詳細は、下記 PaloAlto Networks 社ページをご確認ください。

・PaloAlto Networks 社メーカナレッジ
https://live.paloaltonetworks.com/t5/Community-Blog/UPDATED-Urgent-action-recommended-regarding-recent-security/ba-p/194220

・PaloAlto Networks 社メーカナレッジ（日本語訳）
https://live.paloaltonetworks.com/t5/%E3%83%8A%E3%83%AC%E3%83%83%E3%82%B8%E3%83%89%E3%82%AD%E3%83%A5%E3%83%A1%E3%83%B3%E3%83%88/%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%8B%A7%E5%91%8APAN-SA-2017-0027%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E6%8E%A8%E5%A5%A8%E3%81%95%E3%82%8C%E3%82%8B%E7%B7%8A%E6%80%A5%E5%AF%BE%E5%87%A6%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6/ta-p/194357

(2018/1/19 追記)

以下、PaloAlto Networks 社セキュリティアドバイザリーも合わせてご確認ください。
https://securityadvisories.paloaltonetworks.com/
Vulnerability in PAN-OS and Panorama on Management Interface

以上