２０１９年８月２３日

お客様各位

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

リモートコード実行に繋がる脆弱性(CVE-2019-1581)について

平素は Palo Alto Networks 製品ユーザー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 7.1.24 以前、8.0.19 以前、8.1.9 以前、9.0.3 以前に重要な脆弱性が発見されたため、以下の通りご連絡いたします。

1. 事象内容

   悪用された場合、リモートから認証されていないユーザが悪意のあるメッセージを作成し、任意のコードを実行することができる脆弱性が存在しています。

2. 対象のお客様

   PAN-OS 7.1.24 以前、8.0.19 以前、8.1.9 以前、9.0.3 以前をご利用のお客様

3. 恒久対策

   PAN-OS 7.1.24-h1 以降、8.0.19-h1 以降、8.1.9-h4 以降、9.0.3-h3 以降をご利用ください。

4. 運用回避策

   本脆弱性はPAN-OSの管理インターフェースを保護するためのベストプラクティスに従うことで軽減されます。ネットワークセグメンテーションまたは管理アクセスに制限をかけることが推奨されております。

   下記の PaloAlto Networks 社ページも併せてご参照ください。

   ・管理アクセスを保護するためのベストプラクティス
   https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

以上