２０１９年7月５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

TCP SACK パニックを引き起こす脆弱性(CVE-2019-11477, 11478, 11479)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 7.1.23 以前、8.0.18 以前、8.1.8-h4 以前、9.0.2-h3 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

対象 PAN-OS にて Linux カーネルにおける TCP SACK パニックを引き起こす脆弱性が存在しております。

この問題が悪用された場合、特権を持たないリモートユーザが対象のソフトウェアを実行しているシステムでカーネルパニックを引き起こし、サービス拒否に陥る可能性がございます。

この問題は主に管理プレーン(MP)に影響しますが、サービスルートまたはインターフェース管理プロファイルの設定によっては MP サービスがデータプレーン(DP)インターフェースを介して公開される可能性がございます。例として、WebGUI、SSH、応答ページへの HTTP/HTTPS アクセスを許可する管理プロファイルがございます。

このような場合、悪意のあるトラフィックが DP インターフェースを介して MP カーネルに到達する可能性がございます。

2. 対象のお客様

PAN-OS 7.1.23 以前、8.0.18 以前、8.1.8-h4 以前、9.0.2-h3 以前をご利用のお客様

3. 恒久対策

PAN-OS 7.1.24 以降、8.0.19　以降、8.1.8-h5 以降、9.0.2-h4 以降をご利用ください。

２０１９年７月５日

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