２０２０年5月１５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

Panorama の認証バイパスの脆弱性(CVE-2020-2018)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、Panorama のコンテキスト切り替え機能に認証バイパスの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

   Panorama のコンテキスト切り替え機能に認証バイパスの脆弱性が存在しております。本脆弱性が悪用された場合、Panorama の管理インターフェースにネットワークアクセスできる攻撃者が、管理デバイスに特権アクセス可能となる可能性がございます。

   なお、本脆弱性は Panorama と管理デバイス間の通信にカスタム証明書を使用した認証で構成されている場合は影響ございません。

2. 対象のお客様

   PAN-OS 7.1.26 より前、8.1.12 より前、9.0.6 より前をご利用のお客様
   ※PAN-OS 8.0 は全てのバージョン

3. 恒久対策

   PAN-OS 7.1.26 以降、8.1.12 以降、9.0.6 以降へのバージョンアップをご検討ください。
   ※PAN-OS 8.0 は 2019 年 10 月 31 日をもってメーカサポートが終了しておりますため製品セキュリティ保証ポリシーの対象外となっております。

4. 運用回避策

本脆弱性は、Panorama と管理デバイス間でカスタム証明書を使用した認証を有効にすることで回避することができます。
下記の PaloAlto Networks 社ページも併せてご参照ください。

・カスタム証明書を使用した認証の設定
https://docs.paloaltonetworks.com/panorama/8-0/panorama-admin/set-up-panorama/set-up-authentication-using-custom-certificates.html

また、本脆弱性は Panorama 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。
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

5. その他特記事項

PaloAlto Networks 社からは、2020 年 5 月 13 日に本脆弱性以外にも PaloAlto Networks 社製品に関するセキュリティアドバイザリーが同時に複数発表されております。
（High 17 件、Medium 8 件、Low 1 件, Informational 1 件）
詳しくは弊社サポートサイトのセキュリティアドバイザリーをご参照ください。

・弊社サポートサイトー[技術情報]ー[セキュリティアドバイザリー]
https://csps.hitachi-solutions.co.jp/paloalto/share/tech/tech_info.html#sa

以上