

2020年9月11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

Captive Portal または多要素認証が有効な場合にバッファオーバーフローが発生する脆弱性(CVE-2020-2040)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りまして誠にありがとうございます。

この度、Captive Portal または多要素認証(MFA)が有効な場合にバッファオーバーフローが発生する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

PAN-OS に Captive Portal または多要素認証が(MFA)が有効な場合にバッファオーバーフローが発生する脆弱性が存在しております。

本脆弱性が悪用された場合、認証されていない攻撃者がシステムプロセスを妨害し、Captive Portal や MFA(Multi-Factor Authentication)インターフェースに悪意のあるリクエストを送信することにより、root 権限で任意のコードを実行される可能性があります。

なお、本脆弱性は Captive Portal と多要素認証(MFA)のどちらもご利用されていない場合には影響ございません。また、Global Protect VPN または PAN-OS 管理インターフェースにも影響ございません。

2. 対象のお客様

PAN-OS 8.1.15 より前、9.0.9 より前、9.1.3 より前の PAN-OS バージョンをご利用のお客様

※PAN-OS 8.0 は全てのバージョン

3. 恒久対策

PAN-OS 8.1.15 以降、9.0.9 以降、9.1.3 以降へのバージョンアップをご検討ください。

なお、10.0.0 を含めたそれ以降の全ての PAN-OS バージョンで修正されております。

※PAN-OS 7.1 は 2020 年 6 月 30 日、PAN-OS 8.0 は 2019 年 10 月 31 日をもってメーカーサポートが終了しておりますため Palo Alto Networks 社の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

Contents Version 8317 のシグネチャを適用することで CVE-2020-2040 に対する攻撃がブロックされ本脆弱性を回避することができます。

5. その他特記事項

Palo Alto Networks 社からは、2020 年 9 月 9 日に本脆弱性以外にも Palo Alto 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 5 件、Medium 1 件、Low 2 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－[技術情報]－[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