２０２０年9月１８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（第２報）

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、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ございます。

   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がございません。

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. Captive Portal と多要素認証(MFA)ご利用有無の確認方法

   A) Captive Portal の確認方法
      WebUI [Device ＞ User Identification ＞ Captive Portal Settings]
      上記の設定箇所にて以下いずれかの設定になっている場合は Captive Portal が無効となっております。

・[Enable Captive Portal]にチェックが入っていない。
・[Authentication Profile]または[Certificate Profile]が設定されていない。

B) 多要素認証(MFA)の確認方法
WebUI [Device ＞ Server Profiles ＞ Multi Factor Authentication]
上記の設定箇所にサーバプロファイルがない場合は、多要素認証(MFA)をご利用されておりません。

4. 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。

5. 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。

6. 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