２０１９年9月６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

GlobalProtect Portal/Gateway のインタフェースにリモートコード実行の脆弱性 (CVE-2019-1579)（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。

GlobalProtect の脆弱性(CVE-2019-1579)につきまして、既に弊社サポートサイトでご案内をしておりますが、改めて以下にご案内させていただきます。お客様におかれましては、早急なご対応をご検討ください。

1. 事象内容

GlobalProtect Portal および GlobalProtect Gateway のインタフェースにリモートコード実行(RCE)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、認証されていない攻撃者が任意のコードを実行できる可能性がございます。

2. 対象のお客様

PAN-OS 7.1.18 以前、8.0.11-h1 以前、8.1.2 以前　かつ　GlobalProtect をご利用されているお客様。

※PAN-OS 9.0 は影響ございません。

※GlobalProtect 機能をご利用されていない場合、本脆弱性に該当いたしません。

※GlobalProtect 機能の設定有無につきましては、下記の手順でご確認ください。

① WebUI へログインする。
② Network タブ ＞GlobalProtect へ遷移する。
③ ”Portal(ポータル)”および”Gateway(ゲートウェイ)”より設定有無を確認する。
※デフォルトでは GlobalProtect 機能は無効となっております。

２０１９年9月６日

3. 恒久対策

PAN-OS 7.1.19 以降、8.0.12 以降、8.1.3 以降をご利用ください。

なお、本問題の対策として、上記対策バージョンの利用に加え、下記の作業を実施することをご検討ください。

・機器の FactoryReset

・GlobalProtect へのログインに使用する全てのエンドユーザと管理者のパスワード変更。

・PA/GlobalProtect と連携する LDAP、RADIUS、AD などのパスワード変更。

・証明書署名要求（CSR）の新規生成とデバイス証明書の更新。

4. 運用回避策

以下２つを合わせた回避策をご検討ください。

- ContentsVersion:8173 以降へアップグレードする。
  ※本脆弱性に対応するシグネチャが含まれております。(シグネチャ ID:54582)
- GlobalProtect Portal および GlobalProtect Gateway Interface を通過する通信に対するポリシーに Vulnerability Protection を適用する。
  ※上記シグネチャのデフォルトアクションは”Alert”のため、検知時に Threat ログへ出力はされますが該当通信を遮断する動作とはなりません。
  Vulnerability Protection プロファイルにて遮断動作となるようアクションの変更をご検討ください。

以上