２０１９年7月２６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)

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 7.1.18 以前、8.0.11-h1 以前、8.1.2 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

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。

この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 以前をご利用のお客様。

※PAN-OS 9.0 は影響ございません。

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。

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