２０２０年１１月１３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 SSL VPN にクライアント証明書認証がバイパスされる脆弱性 (CVE-2020-2050)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、Palo Alto Networks 社より GlobalProtect の SSL VPN においてクライアント証明書を使用した認証のバイパスが可能となる脆弱性がアナウンスされましたので、以下の通りご連絡いたします。

1. 脆弱性の概要

   GlobalProtect の SSL VPN においてクライアント証明書を使用した認証のバイパスが可能となる脆弱性が存在しております。
   GlobalProtect Gateway、GlobalProtect Portal、GlobalProtect Clientless VPN がクライアント証明書ベースの認証に完全に依存する構成となっている場合、攻撃者が無効な証明書を使用してクライアント証明書のチェックをバイパスし、制限された VPN ネットワークリソースにアクセス可能となる可能性がございます。
   その他の認証方法は本脆弱性の影響はございません。

2. 対象のお客様

   PAN-OS 8.1.17 より前、9.0.11 より前、9.1.5 より前、10.0.1 より前をご利用かつ、GlobalProtect Gateway、GlobalPortal Portal、GlobalProtect Clientless VPN のいずれかをご利用のお客様。

Versions	影響を受ける	影響を受けない
PAN-OS 10.0	< 10.0.1	>= 10.0.1
PAN-OS 9.1	< 9.1.5	>= 9.1.5
PAN-OS 9.0	< 9.0.11	>= 9.0.11
PAN-OS 8.1	< 8.1.17	>= 8.1.17

3. クライアント証明書を使用した認証のご利用有無の確認方法
   WebUI またはコンフィグファイルからの 2 通りの確認方法がございます。

   A) WebUI からの確認方法
      WebUI [Network タブ > GlobalProtect > Portal / Gateway > Authentication]
      上記設定箇所の Client Authentication 項目にて、Certificate Profile にプロファイルが設定されている場合はクライアント証明書を使用した認証をご利用されております。

   B) コンフィグファイルからの確認方法
      <certificate-profile>にプロファイルが設定されているかをご確認ください。
      下記のようにプロファイル名がある場合、クライアント証明書を使用した認証をご利用されております。

```
<global-protect>
  <global-protect-gateway>
    <entry name="GlobalProtect ゲートウェイ名">
      <certificate-profile>”プロファイル名”</certificate-profile>
    </entry>
  </global-protect-gateway>

  <global-protect-portal>
    <entry name="GlobalProtect ポータル名">
      <portal-config>
        <certificate-profile>”プロファイル名”</certificate-profile>
      </portal-config>
    </entry>
  </global-protect-portal>
</global-protect>
```

4. 恒久対策
   PAN-OS 8.1.17 以降、9.0.11 以降、9.1.5 以降、10.0.1 以降へのバージョンアップをご検討ください。

5. 運用回避策

恒久対策を実施するまでの間、GlobalProtect Gateway、GlobalProtect Portal、GlobalProtect Clientless VPN 宛のトラフィックに対して、Threat ID 59884 のシグネチャを有効にすることで本脆弱性に対しての攻撃が遮断されます。
該当のシグネチャは Contents Version 8343 から有効になっております。

なお、本脆弱性は GlobalProtect Portal および GlobalProtect Gateway を利用するユーザが資格情報で認証をするように構成することで軽減されます。

6. その他特記事項

Palo Alto Networks 社からは、2020 年 11 月 11 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 3 件、Medium 1 件、Low 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