２０２６年6月５日

お客様各位

株式会社日立ソリューションズ
Palo Alto Networks 製品ユーザサポート

GlobalProtect 認証バイパスの脆弱性（CVE-2026-0257)について

平素は Palo Alto Networks 製品ユーザ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 認証バイパスの脆弱性（CVE-2026-0257)について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. 概要

   PAN-OS ソフトウェアの GlobalProtect ポータルおよびゲートウェイに存在する認証バイパスの脆弱性により、攻撃者はセキュリティ制限を回避し、不正に VPN 接続を確立することが可能です。
   該当するお客様におかれましては、PAN-OS ソフトウェアのアップグレードをご検討ください。

2. 対象のお客様および対策バージョン

   対象は表 1 の影響を受ける OS バージョンおよび次ページ記載の構成でご利用されているお客様です。なお、Panorama、Cloud NGFW は当該脆弱性の影響を受けません。

表 1 対象 OS バージョン

OS バージョン	影響を受ける OS バージョン	対策 OS バージョン
PAN-OS 12.1 系	12.1.7 未満	12.1.7 以上
	12.1.2～12.1.4-h6 未満	12.1.4-h6 または 12.1.7 以上
PAN-OS 11.2 系	11.2.12 未満	11.2.12 以上
	11.2.8～11.2.10-h7 未満	11.2.10-h7 または 11.2.12 以上
	11.2.5～11.2.7-h14 未満	11.2.7-h14 または 11.2.12 以上
	11.2.0～11.2.4-h17 未満	11.2.4-h17 または 11.2.12 以上
PAN-OS 11.1 系	11.1.15 未満	11.1.15 以上
	11.1.11～11.1.13-h5 未満	11.1.13-h5 または 11.1.15 以上
	11.1.8～11.1.10-h25 未満	11.1.10-h25 または 11.1.15 以上
	11.1.7～11.1.7-h6 未満	11.1.7-h6 または 11.1.15 以上
	11.1.5～11.1.6-h32 未満	11.1.6-h32 または 11.1.15 以上
	11.1.0～11.1.4-h33 未満	11.1.4-h33 または 11.1.15 以上

PAN-OS 10.2	10.2.17～10.2.18-h6 未満	10.2.18-h6 以上
	10.2.14～10.2.16-h7 未満	10.2.16-h7 または 10.2.18-h6 以上
	10.2.11～10.2.13-h21 未満	10.2.13-h21 または 10.2.18-h6 以上
	10.2.8～10.2.10-h36 未満	10.2.10-h36 または 10.2.18-h6 以上
	10.2.0～10.2.7-h34 未満	10.2.7-h34 または 10.2.18-h6 以上
Prisma Access 11.2	11.2.0～11.2.7-h13 未満	11.2.7-h13 以上
Prisma Access 10.2	10.2.0～10.2.10-h36 未満	10.2.10-h36 以上

※ GlobalProtect ポータルまたはゲートウェイの認証オーバーライド Cookie を使用するように設定されている場合、対策 OS バージョンへのアップグレード後に Cookie が再生成されます。そのため、アップグレード後に一度だけ再認証を行う必要があります。再認証後、認証オーバーライド Cookie は、アップグレード前と同様に機能します。

※ Prisma Access は、お客様に共有したアップグレードスケジュールに従って、すべてのお客様向けにアップグレードを実施していきます。

本脆弱性は、認証オーバーライド Cookie が有効になっている GlobalProtect ポータルまたは GlobalProtect ゲートウェイが構成されている PA シリーズ（VM シリーズ含む）に影響します。

認証オーバーライド Cookie が有効になっているかは、以下の手順で確認できます。

- GlobalProtect ポータル
  1. WebUI にログインし、NETWORK タブ > GlobalProtect > Portals に移動します。
  2. NAME 列にある、設定を確認したいポータルの名前をクリックします。
  3. Agent タブ > Agent にて、CONFIGS 列を参照し、設定を確認したい Agent 設定の名前をクリックします。
  4. Authentication タブ > Authentication Override の設定を確認します。
     以下の設定がすべて実施されている場合、GlobalProtect ポータルで認証オーバーライド Cookie が有効になっています。
     (1). Generate cookie for authentication override または、Accept cookie for authentication override オプションにチェックが入っている。
     (2). Certificate to Encrypt/Decrypt Cookie に証明書が設定されている。

- GlobalProtect ゲートウェイ
  1. WebUI にログインし、NETWORK タブ > GlobalProtect > Gateways に移動します。
  2. NAME 列にある、設定を確認したいゲートウェイの名前をクリックします。
  3. Agent タブ > Client Settings と移動します。
  4. CONFIGS 列を参照し、設定を確認したい Client 設定の名前をクリックします。
  5. Authentication Override タブに移動して設定を確認します。
     以下の設定がすべて実施されている場合、GlobalProtect ゲートウェイで認証オーバーライド Cookie が有効になっています。

(1). Accept cookie for authentication override オプションにチェックが入っている。
(2). Certificate to Encrypt/Decrypt Cookie に証明書が設定されている。

3. 回避策および緩和策

以下のいずれかの対策を講じることで、本脆弱性のリスクを緩和することができます。
ご利用の設定において、以下の変更を実施することをご検討ください。

- 認証オーバーライド Cookie 専用の証明書を使用する
  認証 Cookie 専用の新しい証明書を生成し、GlobalProtect ゲートウェイとポータルの Certificate to Encrypt/Decrypt Cookie へ設定ください。
  ※ GlobalProtect ゲートウェイとポータルの当該箇所には、同じ証明書を設定する必要があります。なお、この証明書を GlobalProtect ポータルまたはゲートウェイの他の設定箇所において再利用することや、他の機能またはユーザと共有することは控えてください。
- 認証オーバーライドを無効化する
  GlobalProtect ポータルおよびゲートウェイの設定で、下記認証オーバーライドオプション（Cookie の生成と受け入れに関するオプション）のチェックを外します。
  ・Generate cookie for authentication override
  ・Accept cookie for authentication override

4. 解決策

対象のお客様は、表 1 の対策 OS バージョンへのアップグレードをご検討ください。

5. よくある質問（FAQ）

Q1）GlobalProtect のすべてのコンポーネントを同時にアップグレードする必要がありますか？
はい。認証オーバーライド Cookie を使用する環境では、Cookie を生成または受け入れるすべての GlobalProtect ポータルおよびゲートウェイ（内部および外部の両方）を、表 1 に記載されている対策 OS バージョンに従ってアップグレードする必要があります。これにより、修正プログラムが環境全体の一部にしか適用されなかった場合に発生する可能性のあるポータルとゲートウェイ間の認証オーバーライド Cookie の互換性の問題を回避できます。

Q2）Prisma Access をハイブリッド構成で展開している場合はどうすればよいですか？
オンプレミスの PA シリーズ（VM シリーズ含む）と Prisma Access のハイブリッド環境において、PA シリーズ（VM シリーズ含む）はすべて、表 1 に記載されている対策 OS バージョンにアップグレードする必要があります。これは、PA シリーズ（VM シリーズ含む）と Prisma Access の環境間の認証オーバーライド Cookie の互換性を維持するために必要です。

Q3）段階的なアップグレード中に、アップグレード済みの GlobalProtect コンポーネントとアップグレードされていない GlobalProtect コンポーネントの間で、認証オーバーライド Cookie の互換性を一時的に維持するにはどうすればよいですか？

複数のバージョンが混在する環境で段階的なアップグレードを実行している場合、以下の CLI コマンドを使用して、アップグレードされた PA シリーズ（VM シリーズ含む）で HMAC 検証を一時的に無効にすることができます。

set global-protect enable-auth-override-cookie-hmac no

これにより、アップグレードされた PA シリーズ（VM シリーズ含む）が従来の Cookie 動作に戻り、移行中のユーザ認証エラーが防止されます。環境内のすべての GlobalProtect ポータルとゲートウェイが対策 OS バージョンにアップグレードされた際は、以下の CLI コマンドを使用して、HMAC 検証を再度有効にする必要があります。

set global-protect enable-auth-override-cookie-hmac yes

Q4）認証オーバーライド Cookie 証明書が以前他のサービスで使用されていた場合、それらのサービスから証明書を削除した後でも、認証オーバーライドのために引き続き使用できますか？

いいえ。証明書が過去に他の機能に使用されていた場合は、安全性を確保するために GlobalProtect ポータルおよびゲートウェイに使用する認証オーバーライド Cookie 専用の新しい証明書を生成する必要があります。

6. その他特記事項

本トピックの詳細や最新情報については、下記の Palo Alto Networks 社ページも併せてご参照ください。

https://security.paloaltonetworks.com/CVE-2026-0257

なお、掲載されている以上の情報は開示されておりません。記載内容以上の情報については、弊社サポートではお答え致しかねますことを予めご了承ください。

以上