２０２１年１２月１０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

# Global Protect ポータルおよびゲートウェイインターフェースのメモリ破壊の脆弱性(CVE-2021-3064)について（12/10 改訂版）

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、Global Protect ポータルおよびゲートウェイのインターフェースにメモリ破壊の脆弱性がある事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. 概要

Global Protect ポータルおよびゲートウェイにメモリ破壊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、認証されていないネットワークベースの攻撃者によりシステムプロセスが妨害され、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、本脆弱性を攻撃者が悪用するには Global Protect インターフェースへのネットワークアクセスが可能な必要があります。

2. 対象のお客様

下記の表で影響を受けるバージョンをご利用されているお客様。

表 2.1 対象 OS バージョン

| OS バージョン | 影響を受ける | 影響を受けない |
|---|---|---|
| Prisma Access 2.2 | None | All |
| Prisma Access 2.1 | None | All |
| PAN-OS 10.1 | None | 10.1.* |
| PAN-OS 10.0 | None | 10.0.* |
| PAN-OS 9.1 | None | 9.1.* |
| PAN-OS 9.0 | None | 9.0.* |
| PAN-OS 8.1 | < 8.1.17 | ≧ 8.1.17 |

・PAN-OS 8.1.17 より前の PAN-OS 8.1 系にのみ影響がございます。
※PAN-OS 8.1.17 は 2020/10/8(PST)にメーカリリースされております。
・Prisma Access をご利用のお客様には影響がございません。

2021/12/10 追記

**・Global Protect をご利用されていないお客様には影響がございません。**

【Global Protect 利用有無の確認手順】

① WebUI にログインする。

② Network > Global Protect > ポータルもしくはゲートウェイに遷移

③ ポータルあるいはゲートウェイにて設定有無を確認する。
設定が無い場合は Global Protect をご利用されていません。
デフォルトでは当該項目は設定されていません。

※下線…追記部分

3. 回避策

Global Protect インターフェース宛のトラフィックに対して、コンテンツバージョン「8486」以降に含まれております Threat ID「91820」と「91855」を適用することで、本脆弱性に関する攻撃の遮断が可能です。

脆弱性防御プロファイルの strict を適用いただくか、または、下表を参考に、手順 A に従い、攻撃を遮断するルール作成をご検討ください。なお、Threat ID「91855」については、ルールのデフォルトアクションが「alert」のため、手順 A でアクションをデフォルトと設定した場合は、検知は可能ですが遮断がされません。遮断を希望される場合は、設定手順 B に従い、例外設定から当該シグネチャのアクションを変更する必要があります。

表 3.1 検出と遮断に必要な Threat ID のシグネチャ情報

| Threat ID | Severity | Default-Action |
|---|---|---|
| 91820 | high | reset-server |
| 91855 | medium | alert |

(コンテンツバージョン「8486」 2021/11/10 メーカリリース時点)

【手順】

A) 本脆弱性の攻撃に対する遮断ルールを設定する手順

① Objects > セキュリティプロファイル > 脆弱性防御に遷移。

② 既存脆弱性防御プロファイルもしくは「追加」をクリック。

③ ルールタブにて当該シグネチャの重大度（Any、もしくは high、medium）にチェックを入れたルールを追加。
※アクションはお客様にてご検討ください。許可/アラートは遮断されません。

④ 脆弱性防御プロファイルをセキュリティポリシールールに適用。

B) 特定 Threat ID のアクションを変更する手順

（A にて medium を含んだルールのアクションをデフォルトに設定した場合）

① Objects > セキュリティプロファイル > 脆弱性防御に遷移。

② A にて編集もしくは新たに追加した脆弱性防御プロファイルを選択。

③ 例外タブにて「全てのシグネチャを表示」をクリックし、アクションを変更するシグネチャの Threat ID を検索。（今回は 91855 を検索）

④ 表示されたシグネチャのアクションを変更して、「有効化」をクリック。

設定変更後にコミットを実行することで設定が反映されます。

なお、本脆弱性に対する攻撃を検出するために SSL 復号化を有効にする必要はございません。

4. 恒久対策

PAN-OS 8.1.17 以降へのバージョンアップをご検討ください。

※PAN-OS 8.1.17 は 2020/10/8(PST)にメーカリリースされております。

PAN-OS 8.1 系最新バージョンは 2021/11/9(PST)メーカリリースの 8.1.21 となります。

5. その他特記事項

Palo Alto Networks 社からは、2021 年 11 月 10 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。（Critical 1 件、High 6 件、Medium 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。

※閲覧には製品ご購入時に同梱されている資料に記載のユーザID/パスワードが必要となります。

・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