２０２４年5月７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

[重要]GlobalProtect における OS コマンドインジェクションの脆弱性(CVE-2024-3400)について(第 8 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。この度、Palo Alto Networks 社より、GlobalProtect における OS コマンドインジェクションの脆弱性(Severity: Critical)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。
Security Advisories が改訂され Device Telemetry の設定有無に関わらず本脆弱性の影響を受ける可能性があることがアナウンスされております。
※　太字箇所は追記もしくは変更箇所となります。

1　概要

対象の PAN-OS バージョンにおいて GlobalProtect 機能が有効になっている場合に、コマンドインジェクションの脆弱性により攻撃者がファイアウォール上の root 権限で任意のコードを実行できる可能性があります。
なお、Cloud NGFW、Panorama アプライアンス、および Prisma Access は本脆弱性の影響を受けません。

2　対象のお客様

下記の表で影響を受ける OS バージョンをご利用されているお客様。

表 1. 影響を受ける 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
Cloud NGFW	None	All
PAN-OS 11.1	11.1.0-h3 未満	11.1.0-h3 以上
	11.1.1-h1 未満	11.1.1-h1 以上
	11.1.2-h3 未満	11.1.2-h3 以上
PAN-OS 11.0	11.0.0-h3 未満	11.0.0-h3 以上
	11.0.1-h4 未満	11.0.1-h4 以上
	11.0.2-h4 未満	11.0.2-h4 以上
	11.0.3-h10 未満	11.0.3-h10 以上
	11.0.4-h1 未満	11.0.4-h1 以上

PAN-OS 10.2	10.2.0-h3 未満	10.2.0-h3 以上
	10.2.1-h2 未満	10.2.1-h2 以上
	10.2.2-h5 未満	10.2.2-h5 以上
	10.2.3-h13 未満	10.2.3-h13 以上
	10.2.4-h16 未満	10.2.4-h16 以上
	10.2.5-h6 未満	10.2.5-h6 以上
	10.2.6-h3 未満	10.2.6-h3 以上
	10.2.7-h8 未満	10.2.7-h8 以上
	10.2.8-h3 未満	10.2.8-h3 以上
	10.2.9-h1 未満	10.2.9-h1 以上
PAN-OS 10.1	None	All
PAN-OS 10.0	None	All
PAN-OS 9.1	None	All
PAN-OS 9.0	None	All
Prisma Access	None	All

※　表は 2024 年 4 月 22 日時点のものです。最新情報につきましては
メーカの Security Advisories をご参照ください。

3　本脆弱性に該当する設定と確認方法

GlobalProtect Gateway または GlobalProtect Portal（もしくはその両方)が有効となっている場合に本脆弱性に該当します。

■確認方法

ファイアウォールの WebUI から([Network] > [GlobalProtect] > [Gateways] または [Network] > [GlobalProtect] > [Portals]）のエントリを確認する。

4　回避策

※　改訂前は Device Telemetry を無効化することにより本脆弱性を回避できる旨を記載しておりましたが、今回 Palo Alto Networks 社から新たに Device Telemetry の有効無効に関わらず本脆弱性の影響を受ける可能性があることがアナウンスされたため回避策から削除しております。

■シグネチャ適用

Threat Prevention のサブスクリプションをお持ちのお客様は、Threat ID 95187、95189 および 95191 (Apps+ Threats 8836-8695 以降で利用可能) を使用して、本脆弱性に対する攻撃をブロックできます。

Threat ID 95187、95189 および 95191 を適用するには、Vulnerability Protection が GlobalProtect インターフェイスに適用されている必要があります。

詳細につきましては後述の手順もしくは下記メーカサイトをご参照ください。

Applying Vulnerability Protection to GlobalProtect Interfaces

https://live.paloaltonetworks.com/t5/globalprotect-articles/applying-vulnerability-protection-to-globalprotect-interfaces/ta-p/340184

【シグネチャ更新】

Apps+Threats 8836-8695 以降が適用されていることを確認ください。

[Dashboard] > [General Information] > Threat Version よりご確認ください。

※未適用の場合は弊社サポートサイトに掲載の下記手順書をご参考に適用ください。

・シグネチャ更新手順書

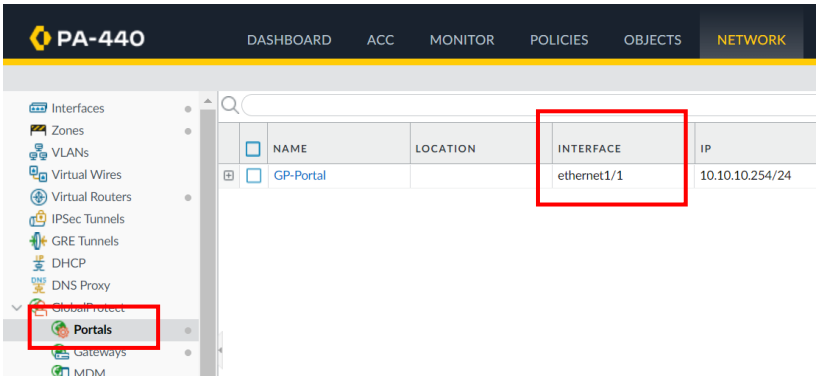
[ダウンロード] > [手順書] > シグネチャ更新手順書

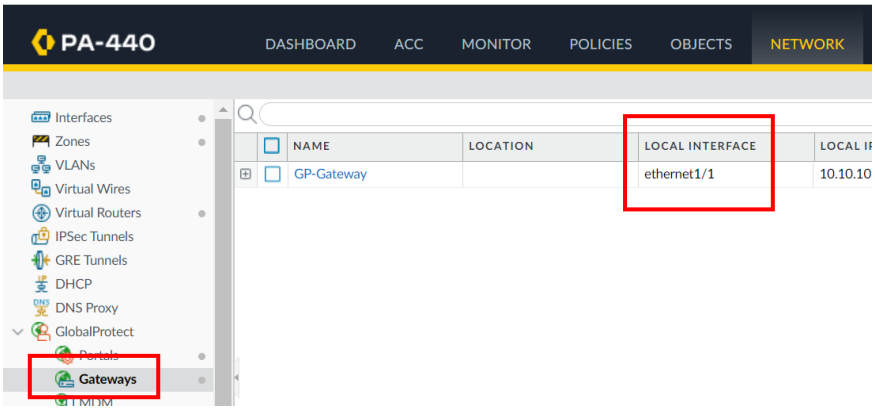
【セキュリティルールの存在有無の確認】

GlobalProtectインターフェース宛通信を識別するためのセキュリティルールの存在有無と Vulnerability Protection Profile が適用されているかを確認します。

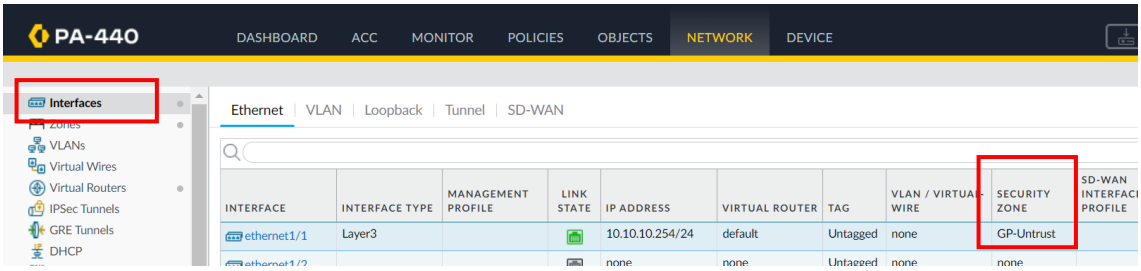
GlobalProtect GatewayおよびPortalは通常インターネット(Untrust側)に公開されているため、Untrust to Untrust が許可されているセキュリティルールを確認します。

1. GlobalProtect Portal および Gateway インターフェースの所属ゾーンを確認。
   ① [Network] > [GlobalProtect] > [Gateways] および [Portals]に遷移。
   ② Gateway および Portal 設定エントリ列の Interface を確認。
   ※例画像の場合”ethernet1/1”となります。





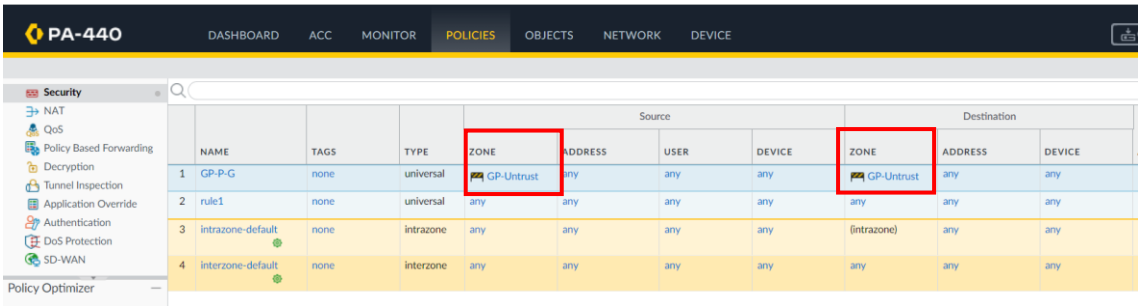
③ [Network] > [Interfaces]にて②で確認した Interface の Security Zone を確認。
※例画像の場合”GP-Untrust”となります。



2. セキュリティルールの存在有無と Vulnerability Protection Profile の適用確認。

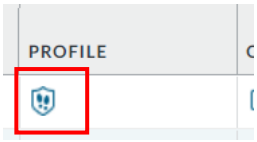
① [Policies] > [Security]に遷移。

② Source Zone および Destination Zone を確認。
1-③で確認した Zone で設定されているルールが存在しているかを確認。
※存在しない場合は”intrazone-default”ポリシーにて識別している可能性があり、その場合は後述の【セキュリティルールが存在しない場合】にて新たにルールを作成する必要がございます。



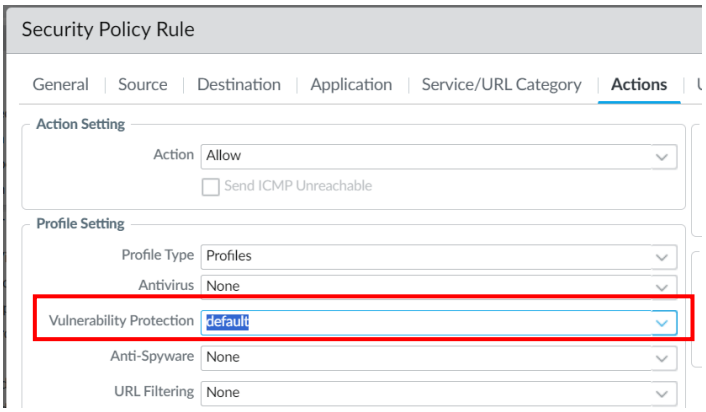
③　（セキュリティルールが存在していた場合）

Profile 列にて Vulnerability Protection Profile の設定有無を確認ください。



④　（Vulnerability Protection Profile が存在していなかった場合）

当該ルールを開いて、[Actions]タブの Profile Setting にて Vulnerability Protection Profile を設定した後に Commit してください。



【セキュリティルールが存在しない場合】

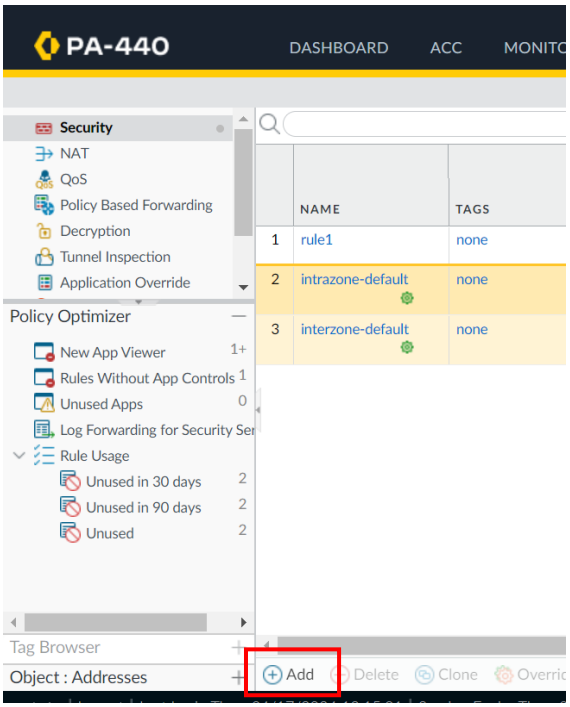
intrazone-default ルールを利用して GlobalProtect インターフェース宛通信を識別している場合には当該デフォルトルールにはプロファイルを設定できないため、新たにルールを作成する必要がございます。

1. セキュリティルールを作成。

※指定されているパラメータ以外はお客様ポリシーに従って設定ください。

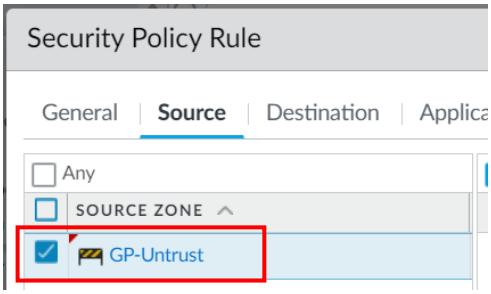
①　[Policies] > [Security]に遷移。

②　Add をクリックして Security Policy Rule 設定ウィンドウを表示。



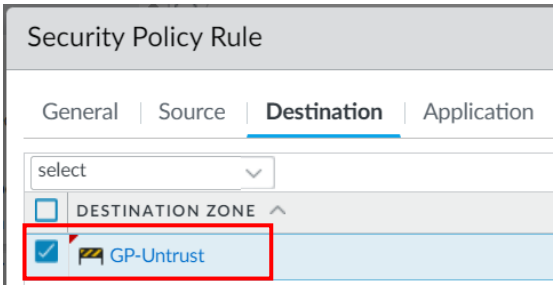
③ Source Zone の設定

[Source]タブにて【セキュリティルールの存在有無の確認】1-③で確認した Security Zone を選択。



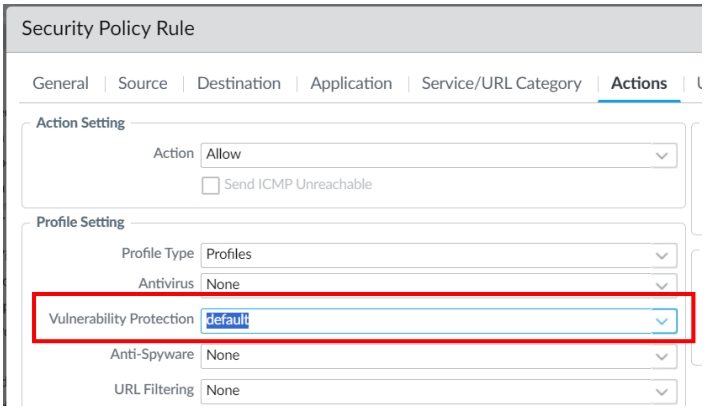
④ Destination Zone の設定

[Destination]タブにて【セキュリティルールの存在有無の確認】1-③で確認した Security Zone を選択。



2. セキュリティルールに Vulnerability Protection Profile を設定。

① [Actions]タブの Profile Setting にて Vulnerability Protection Profile を設定。



② Commit にて設定を適用。

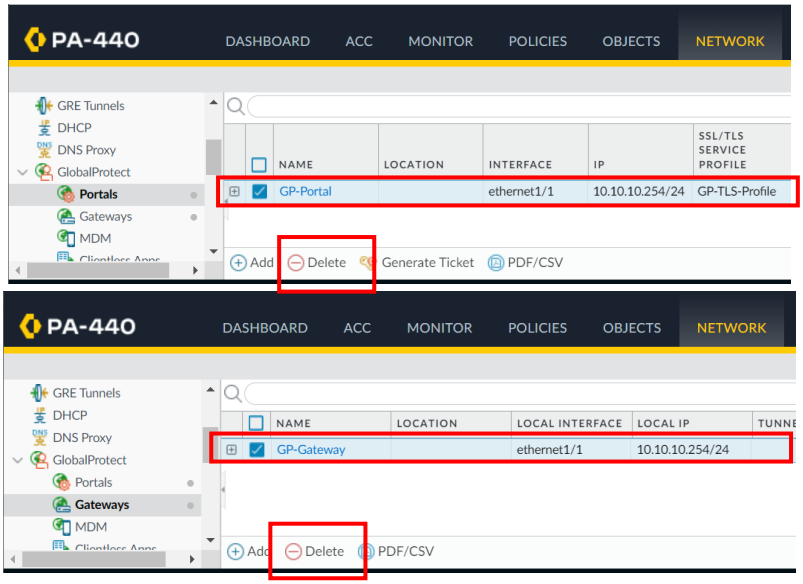
■未利用の GlobalProtect 設定の削除

実際には GlobalProtect 機能を利用していない状況において GlobalProtect Gateway および Portal 設定が残っている場合は設定削除をご検討ください。

【GlobalProtect 設定削除手順】

① [Network] > [GlobalProtect] > [Gateways] および [Portals]に遷移。

② Gateway および Portal 設定エントリを選択。



③ Delete をクリック。

④ Commit にて設定を適用。

5　恒久対策

下記対策 OS バージョンへのアップグレードをご検討ください。

PAN-OS 11.1：

- 11.1.2-h3　(2024/4/14 メーカリリース済み)
- 11.1.1-h1　(2024/4/16 メーカリリース済み)
- 11.1.0-h3　(2024/4/16 メーカリリース済み)

PAN-OS 11.0：

- 11.0.4-h1　(2024/4/14 メーカリリース済み)
- 11.0.4-h2　(2024/4/17 メーカリリース済み)
- 11.0.3-h10　(2024/4/16 メーカリリース済み)
- 11.0.2-h4　(2024/4/16 メーカリリース済み)
- 11.0.1-h4　(2024/4/18 メーカリリース済み)
- 11.0.0-h3　(2024/4/18 メーカリリース済み)

PAN-OS 10.2：

- 10.2.9-h1　(2024/4/14 メーカリリース済み)
- 10.2.8-h3　(2024/4/15 メーカリリース済み)
- 10.2.7-h8　(2024/4/15 メーカリリース済み)
- 10.2.6-h3　(2024/4/16 メーカリリース済み)
- 10.2.5-h6　(2024/4/16 メーカリリース済み)
- 10.2.4-h16　(2024/4/18 メーカリリース済み)
- 10.2.3-h13　(2024/4/18 メーカリリース済み)
- 10.2.2-h5　(2024/4/18 メーカリリース済み)
- 10.2.1-h2　(2024/4/18 メーカリリース済み)
- 10.2.0-h3　(2024/4/18 メーカリリース済み)

※　上述の対策 OS バージョンは 2024 年 4 月 22 日時点のものです。
最新情報につきましてはメーカの Security Advisories をご参照ください。

※　PAN-OS 11.1 につきましては弊社評価中(2024/04/22 時点)です。ハードウェア保守において基本保守サービスのセンドバック、および拡張保守サービスのオンサイト機器交換時に OS 指定が不可となり、テクニカルサポートのみのご提供となります。

なお、各 OS バージョンに対する弊社の最新保守内容については、弊社サポートサイトの下記リリースノートページをご覧ください。
[ダウンロード]>[リリースノート]

6 よくあるご質問

Q1)この問題は実際に悪用されたことがありますか？

Palo Alto Networks 社は、本脆弱性を悪用した攻撃があったことを認識しています。

Q2)本脆弱性の被害に遭ったか確認できますか？

機器の CLI にて下記コマンドを実行してください。
ログが出力されなかった場合や通常時出力例のようなログが出力された場合は攻撃を受けておりません。

コマンド

```
grep pattern "failed to unmarshal session(.¥+.¥/" mp-log gpsvc.log*
```

通常時出力例：

```
failed to unmarshal session(01234567-89ab-cdef-1234-567890abcdef)
```

要調査出力例：

```
failed to unmarshal session(../../some/path)
```

ファイルシステムパスや埋め込みシェルコマンドを含む要調査出力例のようなログが出力された場合は更なる調査が必要な状況となりますため、弊社保守をご契約の場合、テクニカルサポートファイル(TSF)を取得いただき弊社サポート(pa-user@hitachi-solutions.com)までお問い合わせください。弊社にてお客様デバイスのログが本脆弱性の既知の侵害指標(IoC)と一致するかどうか確認いたします。

※ TSF は対策バージョンへのアップグレード実施前に取得してください。アップグレード実施後では以前の稼働バージョンでの一部ログが含まれません。

Q3)本脆弱性の追加情報はどこで確認できますか？

本脆弱性の詳細や最新情報については、Security Advisories、Unit42 の脅威概要ページや Volexity のブログ投稿をご参照ください。なお、下記で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。

Security Advisories
CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect
https://security.paloaltonetworks.com/CVE-2024-3400

Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400
https://unit42.paloaltonetworks.com/cve-2024-3400/

Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

Q4）顧客がクラウド上に展開および管理している VM シリーズは影響を受けますか？
Cloud NGFW は影響を受けませんが、クラウド上で顧客によって展開および管理されている VM シリーズは本脆弱性の影響を受けます。

Q5）本脆弱性の影響があった場合の対処法はありますか？
Palo Alto Networks 社から脆弱性によるデバイスの侵害レベルと、レベルに対応した推奨される対処法が公開されております。

「6.よくあるご質問」Q2 にて要調査出力例に合致して弊社サポートまでお問い合わせを頂いた際には、後述の侵害レベルと詳細な対処法を個別にご案内しております。

表 2.侵害レベルと推奨対処法

侵害レベルと概要	推奨される対処法
レベル 0 - Probe 脆弱性の利用痕跡なし。	・対策 OS へのアップグレード
レベル 1 - Test 脆弱性が試行されている。0 byte ファイルが作成されて常駐しているが、不正コマンド実行の兆候はない。	・対策 OS へのアップグレード
レベル 2 - Potential Exfiltration デバイス上のファイルが Web リクエストを介してアクセス可能な位置にコピーされている。 ※一般的にコピーが確認されているのは running-config.xml	・対策 OS へのアップグレード ・プライベートデータリセット
レベル 3 - Interactive access	・対策 OS へのアップグ

対話型コマンドが実行されている。 シェルベースバックドア/コード導入/ファイルダウンロード/コマンド実行が含まれている場合がある。	レード ・ファクトリーリセット

詳細は下記メーカナレッジをご参照ください。
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CrO6CAK

Q6) Threat Prevention のシグネチャが正しく適用されたことを確認できますか？
GlobalProtect 機能が有効になっている PAN-OS 10.2 以上の PA シリーズに対して Windows のコマンドプロンプトから下記コマンドを実行してください。

コマンド

```
curl -v -k -H "Cookie: SESSID=/../TESTVULN" https://<target-host>/global-protect/login.esp
```

コマンドを実行して応答が無く TCP コネクションがリセットされた場合は、Threat Prevention のシグネチャが正しく適用されていることを示しています。
コマンドを実行して html データが展開された場合は、Threat Prevention のシグネチャが適用されていないことを示しています。「4　回避策」に記載されている内容を実行してください。

7　その他特記事項

Palo Alto Networks 社からは、2024 年 4 月 11 日に本脆弱性以外にも Palo Alto Networks 社製品に関する Security Advisories が複数発表されております。（High 4 件、Medium 3 件、Info 1 件）
詳細につきましては、下記メーカサイトをご参照ください。

Security Advisories
https://security.paloaltonetworks.com/

以上