２０２４年4月１７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 2 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	<11.1.2-h3	≧11.1.2-h3
PAN-OS 11.0	<11.0.4-h1	≧11.0.4-h1
PAN-OS 10.2	<10.2.9-h1	≧10.2.9-h1
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 12 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。本脆弱性に該当する。

4　回避策

■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

※　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。

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。

表 2. 対策 OS バージョン

対象 OS バージョン	対策 OS バージョン
Cloud NGFW	All
PAN-OS 11.1	≧11.1.2-h3
PAN-OS 11.0	≧11.0.4-h1
PAN-OS 10.2	≧10.2.9-h1
PAN-OS 10.1	All
PAN-OS 10.0	All
PAN-OS 9.1	All
PAN-OS 9.0	All
Prisma Access	All

※　表は 2024 年 4 月 12 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。

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？

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。弊社にてメーカケースをオープンし、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。

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。

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