２０２６年２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 製品ユーザサポート

GlobalProtect を利用したサービス拒否(DoS)の脆弱性(CVE-2026-0227)についてのお知らせ（第 2 報）

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 を利用したサービス拒否(DoS)の脆弱性(CVE-2026-0227)についてのお知らせ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。

※　太字箇所は追記もしくは変更箇所となっております。

1. 概要

PAN-OS ソフトウェアの脆弱性により、攻撃者がファイアウォールに対してサービス拒否（DoS）攻撃を仕掛けることが可能です。この状態を繰り返し行うことで、PAN-OS はメンテナンスモードに移行します。

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 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
Cloud NGFW	None	All
PAN-OS 12.1	12.1.3-h3 未満、12.1.4 未満	12.1.3-h3 以上、12.1.4 以上
PAN-OS 11.2	11.2.4-h15 未満、11.2.7-h8 未満、11.2.10-h2 未満	11.2.4-h15 以上、11.2.7-h8 以上、11.2.10-h2 以上
PAN-OS 11.1	11.1.4-h27 未満、11.1.6-h23 未満、11.1.10-h9 未満、11.1.13 未満	11.1.4-h27 以上、11.1.6-h23 以上、11.1.10-h9 以上、11.1.13 以上
PAN-OS 10.2	10.2.7-h32 未満、**10.2.10-h31** 未満、10.2.13-h18 未満、10.2.16-h6 未満、10.2.18-h1 未満	10.2.7-h32 以上、**10.2.10-h31** 以上、10.2.13-h18 以上、10.2.16-h6 以上、10.2.18-h1 以上
PAN-OS 10.1	10.1.14-h20 未満	10.1.14-h20 以上
Prisma Access 11.2	11.2.7-h8 未満*1	11.2.7-h8 以上*1

Prisma Access 10.2	**10.2.4-h43 未満***1、10.2.10-h29 未満*1	**10.2.4-h43 以上***1、10.2.10-h29 以上*1

***1 Palo Alto Networks 社より、Prisma Access のアップグレードが全てのお客様環境において正常に完了した旨、アナウンスがありました。**

3. 本脆弱性に該当する構成

   GlobalProtect ゲートウェイまたはポータルが有効になっている PAN-OS または Prisma Access が影響を受けます。

4. 解決策

   対象のお客様は、下記 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　修正に対応している OS バージョン

OS バージョン	対象 OS バージョン	修正 OS バージョン
Cloud NGFW All	None	All
PAN-OS 12.1	12.1.2～12.1.3	12.1.4 以上
PAN-OS 11.2	11.2.8～11.2.10	11.2.10-h2 以上
	11.2.5～11.2.7	11.2.7-h8 または、11.2.10-h2 以上
	11.2.0～11.2.4	11.2.4-h15 または、11.2.10-h2 以上
PAN-OS 11.1	11.1.11～11.1.12	11.1.13 以上
	11.1.7～11.1.10	11.1.10-h9 または、11.1.13 以上
	11.1.5～11.1.6	11.1.6-h23 または、11.1.13 以上
	11.1.0～11.1.4	11.1.4-h27 または、11.1.13 以上
PAN-OS 10.2	10.2.17～10.2.18	10.2.18-h1 以上
	10.2.14～10.2.16	10.2.16-h6 または、10.2.18-h1 以上
	10.2.11～10.2.13	10.2.13-h18 または、10.2.18-h1 以上
	10.2.8～10.2.10	**10.2.10-h31** または、10.2.18-h1 以上
	10.2.0～10.2.7	10.2.7-h32 または、10.2.18-h1 以上
PAN-OS 10.1	10.1.0～10.1.14	10.1.14-h20 以上
End-of-Life を迎えた OS バージョン	All	サポートされている修正 OS バージョンにアップグレードしてください。
Prisma Access 11.2	11.2.7-h8 未満	11.2.7-h8 以上*1
Prisma Access 10.2	10.2.10-h29 未満	10.2.10-h29 以上*1

***1 Palo Alto Networks 社より、「Prisma Access のアップグレードを全てのお客様において正常に完了しました」とアナウンスがありました。**

5. 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-2026-0227

※　参照には CSP アカウントを所有している必要があります。

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