２０２６年２月２０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

Advanced DNS Security 機能を利用したサービス拒否(DoS)の脆弱性(CVE-2026-0229)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 Advanced DNS Security 機能を利用したサービス拒否(DoS)の脆弱性(CVE-2026-0229)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

Advanced DNS Security 機能に存在するサービス拒否(DoS)の脆弱性により、攻撃者が悪意のあるパケットを使用して PAN-OS ソフトウェアの再起動を実行できます。再起動を繰り返し実行すると、ファイアウォール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	12.1.4 未満	12.1.4 以上
PAN-OS 11.2	11.2.10 未満	11.2.10 以上
PAN-OS 11.1	None	All
PAN-OS 10.2	None	All
Panorama	**None**	**All**
Prisma Access	None	All

3. 本脆弱性に該当する構成

本脆弱性の影響を受けるのは、以下の条件を満たす場合です。

- ファイアウォールで Advanced DNS Security が有効になっている
- 「block」「sinkhole」「alert」のいずれかの値を実行するようにアクションが構成されたスパイウェアプロファイルが設定されている

4. 脅威活動

Palo Alto Networks 社は、本脆弱性を悪用した事例は認識しておりません。

5. 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	None	All
PAN-OS 12.1	12.1.2～12.1.3	12.1.4 以上
PAN-OS 11.2	11.2.0～11.2.9	11.2.10 以上
PAN-OS 11.1	None	All
PAN-OS 10.2	None	All
Panorama	**None**	**All**
Prisma Access	None	All

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-2026-0229

※　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