２０２６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 製品ユーザサポート

User-ID 認証ポータルサービスを利用した脆弱性(CVE-2026-0300)についてのお知らせ

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 User-ID™認証ポータルサービスを利用した脆弱性(CVE-2026-0300)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。

1. 概要

PAN-OS ソフトウェアの User-ID™認証ポータル（旧キャプティブポータル）サービスには、攻撃者が細工したパケットを送信することで発生するバッファオーバーフローの脆弱性が存在します。この脆弱性を利用された場合、PA シリーズ（VM シリーズ含む）において、ルート権限で任意のコードが実行される可能性があります。

2. 対象のお客様と対策バージョン

下記の影響を受ける OS バージョンを、影響を受ける構成でご利用されているお客様。

表 1 対象 OS バージョン

対象製品	影響を受ける OS バージョン	対策 OS バージョン
Cloud NGFW	-	全バージョン
PAN-OS 12.1	12.1.4-h5 未満 12.1.7 未満	12.1.4-h5 以上*1 12.1.7 以上*2
PAN-OS 11.2	11.2.4-h17 未満 11.2.7-h13 未満 11.2.10-h6 未満 11.2.12 未満	11.2.4-h17 以上*2 11.2.7-h13 以上*1 11.2.10-h6 以上*1 11.2.12 以上*2
PAN-OS 11.1	11.1.4-h33 未満 11.1.6-h32 未満 11.1.7-h6 未満 11.1.10-h25 未満 11.1.13-h5 未満 11.1.15 未満	11.1.4-h33 以上*1 11.1.6-h32 以上*1 11.1.7-h6 以上*2 11.1.10-h25 以上*1 11.1.13-h5 以上*1 11.1.15 以上*2

PAN-OS 10.2	10.2.7-h34 未満 10.2.10-h36 未満 10.2.13-h21 未満 10.2.16-h7 未満 10.2.18-h6 未満	10.2.7-h34 以上*2 10.2.10-h36 以上*1 10.2.13-h21 以上*2 10.2.16-h7 以上*2 10.2.18-h6 以上*1
Prisma Access	-	全バージョン

*1　2026 年 5 月 13 日メーカリリース予定

*2　2026 年 5 月 28 日メーカリリース予定

当該事象の影響を受けるのは、以下の両方の条件を満たしている場合です。

- User-ID 認証ポータルが有効になっている場合。
  - ※ Device > User Identification > Authentication Portal Settings > Enable Authentication Portal に移動して構成を確認できます。
- 外部ネットワークから到達可能な Ethernet ポートに設定済の管理プロファイル（MANAGEMENT PROFILE）において、応答ページ（Response Pages）を有効にしている場合。
  - ※ 管理プロファイル（MANAGEMENT PROFILE）の設定は、NETWORK > Network Profiles > Interface Mgmt にて表示される設定済の管理プロファイルの一覧から確認できます。

信頼できない IP アドレスや外部ネットワークに公開されている User-ID™認証ポータルを標的とした、限定的な攻撃が確認されています。User-ID™認証ポータルの公開先を信頼できる内部ネットワークに限定するなど、標準的なセキュリティのベストプラクティスを実施しているお客様は、リスクを大幅に軽減できます。

3. 回避策

以下のいずれかの対策を講じることで、本脆弱性のリスクを軽減できます。

- User-ID™認証ポータルへのアクセスを信頼できるゾーンのみに制限し、信頼できないトラフィックやインターネットトラフィックが流入する可能性のあるゾーンの L3 インターフェイスに設定されているインターフェイス管理プロファイルの応答ページを無効にします。応答ページは、正当なユーザーのブラウザーが流入する信頼ゾーン/内部ゾーンのインターフェイスでのみ有効にします。本手順につきましては、下記メーカナレッジベースのステップ 6 をご参照ください。なお、参照には CSP アカウントを所持している必要があります。

  How to Configure Captive Portal
  https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CqbiCAC
- 不要な場合は、User-ID™認証ポータルを無効にすることをご検討ください。
- Threat Prevention サブスクリプションをご利用中且つ、PAN-OS11.1 以降をご利用中のお客様は Threat ID 510019（Applications and Threats content version 9097 で導入）を有効にすることで本脆弱性に対する攻撃をブロックすることができます。

4. 解決策

対象のお客様は、表 1 の対策 OS バージョンへのアップグレードをご検討ください。

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-2026-0300
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