２０２６年5月１８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

PAN-OS でのクラウド認証サービス有効化による認証バイパスの脆弱性(CVE-2026-0265)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 PAN-OS ソフトウェアにおけるクラウド認証サービス(CAS)有効化による認証バイパスの脆弱性(CVE-2026-0265)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。

1. 概要

PAN-OS ソフトウェアにおける認証バイパスの脆弱性により、クラウド認証サービス(CAS)が有効化されている場合、攻撃者が認証制御を回避できるようになります。該当するお客様におかれましては、PAN-OS ソフトウェアのアップグレードをご検討ください。

2. 対象のお客様と対策バージョン

対象は表 1 の影響を受ける OS バージョンおよび構成でご利用されているお客様です。なお、Cloud NGFW および Prisma Access は当該脆弱性の影響を受けません。

表 1 対象 OS バージョン

OS バージョン	影響を受ける OS バージョン	対策 OS バージョン
PAN-OS 12.1 系	12.1.5～12.1.6	12.1.7※以上
	12.1.2～12.1.4-h*	12.1.4-h5 または 12.1.7※以上
PAN-OS 11.2 系	11.2.12 未満	11.2.12※以上
	11.2.8～11.2.10-h*	11.2.10-h6 または 11.2.12※以上
	11.2.5～11.2.7-h*	11.2.7-h13 または 11.2.12※以上
	11.2.0～11.2.4-h*	11.2.4-h17※または 11.2.12※以上
PAN-OS 11.1 系	11.1.15 未満	11.1.15※以上
	11.1.11～11.1.13-h*	11.1.13-h5 または 11.1.15※以上
	11.1.8～11.1.10-h*	11.1.10-h25 または 11.1.15※以上
	11.1.7～11.1.7-h*	11.1.7-h6※または 11.1.15※以上
	11.1.5～11.1.6-h*	11.1.6-h32 または 11.1.15※以上
	11.1.0～11.1.4-h*	11.1.4-h33 または 11.1.15※以上

PAN-OS 10.2	10.2.17～10.2.18-h*	10.2.18-h6 以上
	10.2.14～10.2.16-h*	10.2.16-h7 または 10.2.18-h6 以上
	10.2.11～10.2.13-h*	10.2.13-h21 または 10.2.18-h6 以上
	10.2.8～10.2.10-h*	10.2.10-h36 または 10.2.18-h6 以上
	10.2.0～10.2.7-h*	10.2.7-h34※または 10.2.18-h6 以上

※　5/28(米国時間)に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構成です。

・ 認証プロファイル(Authentication Profile)において、認証方式が Cloud Authentication Service(CAS)に設定されているプロファイルがある場合。

※ DEVICE > Authentication Profile へ移動して、画面上のプロファイル一覧より、認証方式(AUTHENTICATION)の設定を確認できます。

・ 下記の設定箇所で、CAS を認証方式とした Authentication Profile が適用されている場合。

DEVICE タブ

1. Setup > Management > Authentication Settings > Authentication Profile
2. User Identification > Authentication Portal Settings > Authentication Portal > Authentication Profile

NETWORK タブ

GlobalProtect > Gateways へ移動して、以下の通りご確認ください。

1. 確認対象の Gateway 設定をクリックする。
2. Authentication > Client Authentication から、確認対象のクライアント認証設定をクリックする。
3. Authentication Profile の設定を確認する。

GlobalProtect > Portals へ移動して、以下の通りご確認ください。

1. 確認対象の Portal 設定をクリックする。
2. Authentication > Client Authentication から、確認対象のクライアント認証設定をクリックする。
3. Authentication Profile の設定を確認する。

・ Strata Cloud Manager をご利用のお客様は下記の設定もご確認ください。

1. Configuration > NGFW and Prisma Access > Identity Services > Authentication へ移動する。
2. Authentication Profile にて、CAS(Cloud Identity Engine)を利用する設定の有無を確認する。

上記設定を確認した結果、Cloud Identity Engine を利用する設定が存在する場合は、以下の設定も併せてご確認ください。

1. Configuration > NGFW and Prisma Access へ移動する。
2. Device > Device Setup > Authentication and Accounting Settings > Authentication profile にて、CAS(Cloud Identity Engine)を利用する Authentication Profile が指定されているかご確認ください。

クラウド認証サービス(CAS)が有効になっているかを確認する方法につきましては、下記メーカドキュメントも併せてご参照ください。

Next-Generation Firewall

https://docs.paloaltonetworks.com/ngfw/help/10-2/device/device-authentication-profile/configure-an-authentication-profile

3. 回避策および緩和策

以下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。

- 管理インターフェイスへのアクセスを信頼できる内部 IP アドレスのみに制限する。詳細な手順につきましては、下記メーカドキュメントおよびメーカコミュニティをご参照ください。

  Administrative Access Best Practices
  https://docs.paloaltonetworks.com/best-practices/10-1/administrative-access-best-practices/administrative-access-best-practices/deploy-administrative-access-best-practices

  How to Secure the Management Access to your Palo Alto Networks Device
  https://live.paloaltonetworks.com/t5/community-blogs/critical-recommendations-for-deployment-guides-how-to-secure-the/ba-p/464431
- 対象となる認証プロファイルを SAML、RADIUS、またはその他のサポートされている認証方法に変更することで、クラウド認証サービス(CAS)を無効にすることができます。
- Threat Prevention サブスクリプションをご利用中かつ、PAN-OS11.2 以降をご利用中のお客様は Threat ID 510008（Applications and Threats content version 9100 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-2026-0265

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