２０２６年7月１０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

Terminal Server Agent におけるバッファオーバーフローの脆弱性 (CVE-2026-0288)について

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 Terminal Server Agent におけるバッファオーバーフローの脆弱性(CVE-2026-0288)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 ソフトウェアの User-ID Terminal Server Agent コンポーネントには複数のバッファオーバーフローの脆弱性があり、攻撃者は外部ネットワークを経由して DoS 攻撃を引き起こすことや、細工されたパケットを送信することで、任意のコード実行を行える可能性があります。
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. 対象のお客様および対策バージョン

対象は表 1 の影響を受ける OS バージョンおよび次ページ記載の構成でご利用されているお客様です。なお、Panorama、Cloud NGFW (AWS および Azure 環境) 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	12.1.5～12.1.7-h2 未満	12.1.7-h2 または 12.1.8 以上
	12.1.2～12.1.4-h8 未満	12.1.4-h8 または 12.1.8 以上
PAN-OS 11.2 系	11.2.11～11.2.13 未満	11.2.13 以上
	11.2.8～11.2.10-h12 未満	11.2.10-h12 または 11.2.13 以上
	11.2.5～11.2.7-h18 未満	11.2.7-h18 または 11.2.13 以上
	11.2.0～11.2.4-h20 未満	11.2.4-h20 または 11.2.13 以上
PAN-OS 11.1 系	11.1.14～11.1.16 未満	11.1.16 以上
	11.1.11～11.1.13-h9 未満	11.1.13-h9 または 11.1.16 以上
	11.1.8～11.1.10-h30 未満	11.1.10-h30 または 11.1.16 以上
	11.1.7～11.1.7-h8 未満	11.1.7-h8 または 11.1.16 以上
	11.1.5～11.1.6-h35 未満	11.1.6-h35 または 11.1.16 以上
	11.1.0～11.1.4-h35 未満	11.1.4-h35 または 11.1.16 以上

PAN-OS 10.2	10.2.17～10.2.18-h8 未満	10.2.18-h8 以上
	10.2.14～10.2.16-h9 未満	10.2.16-h9 以上
	10.2.11～10.2.13-h23 未満	10.2.13-h23 以上
	10.2.8～10.2.10-h39 未満	10.2.10-h39 以上
	10.2.0～10.2.7-h36 未満	10.2.7-h36 以上
Prisma Access 11.2 系	11.2.0～11.2.7-h18 未満	11.2.7-h18 以上※
Prisma Access 10.2 系	10.2.0～10.2.10-h39 未満	10.2.10-h39 以上※

※ Palo Alto Networks 社は、Prisma Access の次回の定期メンテナンス期間中にすべてのお客様のソフトウェアをアップグレードいたします。

本脆弱性の影響を受けるのは、Terminal Server Agent が有効になっている PA シリーズ（VM シリーズ含む）のみです。Terminal Server Agent の設定が有効になっているかは、下記手順で確認できます。後述のメーカドキュメントも併せてご参照ください。

1. Device > User Identification > Terminal Server Agents に移動する。
2. 任意の Terminal Server Agent を選択する。
3. Enabled にチェック(✓)が付いている場合、Terminal Server Agent が有効である。

Device > User Identification > Terminal Server Agents
https://docs.paloaltonetworks.com/ngfw/help/12-1/user-identification/device-user-identification-terminal-services-agents

3. 回避策および緩和策

Terminal Server Agent の接続を信頼できる内部 IP アドレスのみに制限することで本脆弱性のリスクを緩和することができます。
ご利用の設定において、以下の変更を実施することをご検討ください。後述のメーカドキュメントも併せてご参照ください。

1. Device > User Identification > Terminal Server Agents に移動する。
2. 任意の Terminal Server Agent を選択する。
3. Host に信頼できる IP アドレスを設定する。

Device > User Identification > Terminal Server Agents
https://docs.paloaltonetworks.com/ngfw/help/12-1/user-identification/device-user-identification-terminal-services-agents

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-2026-0288

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