２０２６年１０月２９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

Brotli の脆弱性（CVE-2026-111497）の Palo Alto Networks 製品への影響（第 3 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 Brotli に存在する重大な脆弱性による同社製品への影響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。

※ 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

   Brotli のデコーダにおいて、バッファオーバーフローの脆弱性（CVE-2026-111497）が報告されています。また、Palo Alto Networks 社より、PA シリーズ（VM シリーズを含む）および Prisma Cloud が本脆弱性の影響を受けることが確認されています。
   該当するお客様は、対策バージョンのリリース後、アップグレードをご検討ください。
   ※Panorama（M シリーズを含む）は本脆弱性の影響を受けません。
   ※Prisma Cloud の詳細は、同社セキュリティアドバイザリを参照ください。

2. 影響を受ける機能

   Brotli 圧縮トラフィックの検査機能（以下、Brotli 検査機能）、およびデータプレーン上での TLS/SSL 復号が有効な PA シリーズ（VM シリーズを含む）が本脆弱性の影響を受けます。なお、管理用 Web インタフェース（WebUI、XML API サービス）含むは本脆弱性の影響を受けません。

   Brotli 検査機能の有無は、CLI から下記手順で確認できます。
   ① PA シリーズ（VM シリーズを含む）へ CLI でログインします。
   ② ”show system setting brotli”又は”show system setting brotli-encoding”コマンドを実行します。
   ③ Enabled: yes と表示される場合、Brotli 検査機能が有効になっています。

3. 影響を受けるバージョンおよび対策バージョン

以下、表 1 の影響を受けるバージョンで稼働している PA シリーズ（VM シリーズを含む）が本脆弱性の影響を受けます。

表 1　対象および対策 PAN-OS バージョン

PAN-OS バージョン※1	影響を受けるバージョン	対策バージョン	リリース予定日※2
PAN-OS 12.2 系	12.2.4-h1 未満	12.2.4-h1	リリース済
PAN-OS 12.1 系	12.1.10-h3 未満	**12.1.10-h3**	**リリース済**
	12.1.7-h11 未満	12.1.7-h11	リリース済
	12.1.4-h13 未満	**12.1.4-h13**	**リリース済**
PAN-OS 11.2 系	11.2.16-h1 未満	11.2.16-h1	リリース済
	11.2.13-h4 未満	11.2.13-h4	リリース済
	11.2.10-h17 未満	11.2.10-h17	リリース済
	11.2.7-h23 未満	11.2.7-h23	リリース済
	11.2.4-h23 未満	**11.2.4-h23**	**リリース済**
PAN-OS 11.1 系	影響なし	－	－
PAN-OS 10.2 系	影響なし	－	－

※1 PAN-OS 10.1 系未満の OS はサポート終了済みの為、本アナウンスの対象に含まれていません。本表の対策バージョンへの移行をご検討ください。

※2 日付は米国時間を基準にしています。

4. 解決策

対象のお客様は、表 1 対策バージョンへのアップグレードをご検討ください。

5. 緩和策

Palo Alto Networks 社からはワークアラウンド/緩和策として、Brotli 検査機能を無効化する方法および Threat Prevention を利用した方法がアナウンスされています。

CLI から下記手順を実行することで、Brotli 検査機能を無効化できます。

① PA シリーズ（VM シリーズを含む）へ CLI でログインします。
② “set system setting brotli-encoding disable”コマンドを実行します。
③ ”show system setting brotli”又は”show system setting brotli-encoding”コマンドを実行します。
④ Enabled: no と表示された場合、Brotli 検査機能は無効になっています。

その他詳細は、同社セキュリティアドバイザリを参照ください。

6. その他特記事項

本トピックの詳細や最新情報は、下記のセキュリティアドバイザリを参照ください。

https://security.paloaltonetworks.com/CVE-2026-111497

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は、弊社サポートではお答えいたしかねますことをあらかじめご了承ください。

以上