TLP:CLEAR【全分野】

別紙

2026 年 6 月 1 日

内閣官房　国家サイバー統括室
対処調整・官民連携等ユニット

Palo Alto Networks 製品の深刻な脆弱性(CVE-2026-0257)について（注意喚起）

1. 対象ソフトウェア

以下に示すバージョン未満のものが該当します。

- PAN-OS 12.1: 12.1.4-h6 / 12.1.7
- PAN-OS 11.2: 11.2.4-h17 / 11.2.7-h14 / 11.2.10-h7 / 11.2.12
- PAN-OS 11.1: 11.1.4-h33 / 11.1.6-h32 / 11.1.7-h6 / 11.1.10-h25 / 11.1.13-h5 / 11.1.15
- PAN-OS 10.2: 10.2.7-h34 / 10.2.10-h36 / 10.2.13-h21 / 10.2.16-h7 / 10.2.18-h6
- Prisma Access 11.2.0: 11.2.7-h13
- Prisma Access 10.2.0: 10.2.10-h36

2. 脆弱性悪用による影響等

対象ソフトウェアには、GlobalProtect ポータルおよびゲートウェイにおける認証バイパスの脆弱性があり、特定の構成の場合、攻撃者は認証を回避して不正な VPN 接続を確立し、内部ネットワークにアクセスできる可能性があります。

3. 悪用状況

CVE-2026-0257 は、CISA が提供する KEV カタログに追加されており、実際に悪用されていることが確認されています（参考 URL①）。

4. 対応

開発元が提供する情報をもとに脆弱性が修正されたバージョンへのアップグレードを強く推奨します（参考 URL②）。

5. 緩和策

開発元より緩和策が提示されており、即座のアップグレードの実施が難しい場合には、当該緩和策を実施することで、本脆弱性のリスクを軽減できます（参考 URL②）。ただし、ソフトウェアの健全性維持の観点からも、早期のアップグレードを強く推奨します。

参考 URL

① CISA Adds One Known Exploited Vulnerability to Catalog(2026/5/29)
https://www.cisa.gov/news-events/alerts/2026/05/29/cisa-adds-one-known-exploited-vulnerability-catalog

② CVE-2026-0257 PAN-OS: GlobalProtect Authentication Bypass Vulnerabilities (Palo Alto Networks 社)
https://security.paloaltonetworks.com/CVE-2026-0257