PAN-OS GlobalProtect Gatewayにおけるコマンドインジェクションの脆弱性（CVE-2024-3400）

令和6年4月15日
国土交通省 最高情報セキュリティアドバイザー
北尾　辰也

2024年4月12日（現地時間）、Palo Alto Networksは、FW向けOSであるPAN-OSのリモートアクセス機能であるGlobalProtect Gatewayにおけるコマンドインジェクションの脆弱性CVE-2024-3400を公表しました。同社によると、脆弱性の公表時点で悪用が複数確認されているとのことで、JPCERT/CCからも注意喚起が発出されています。また、既に、本脆弱性を悪用する活動が増加しているという情報もあります。

＜脆弱性の内容＞
GlobalProtect Gateway機能におけるコマンドインジェクションの脆弱性。この脆弱性によって、リモートの認証されていない攻撃者が、root権限で任意のコードを実行できる可能性があるもの。
CVSS Base Score: CVSSv3 10.0 （CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H）

＜影響を受けるバージョン＞
- PAN-OS 11.1：11.1.2-h3より前のバージョン
- PAN-OS 11.0：11.0.4-h1より前のバージョン
- PAN-OS 10.2：10.2.9-h1より前のバージョン

＜影響を受ける条件＞
GlobalProtect Gatewayとデバイステレメトリの両方が有効

＜対策＞
ホットフィックス（10.2.9-h1, 11.0.4-h1, 11.1.2-h3）の適用
※4月14日にリリース予定と発表されたが、日本時間 4/15午前の時点ではリリースされていない

＜緩和策＞
デバイステレメトリの無効化
脅威ID 95187の有効化（脅威対策サブスクリプションを導入している場合のみ）

＜侵害有無の確認方法＞
Customer Support Portal （CSP）にてtechnical support file（TSF）をアップロードし既知のIoC（Indicators of Compromise）情報と突合する

＜コメント＞
影響を受けるバージョンの機器を外部に公開している場合、以下の対応を実施下さい。
1. GlobalProtect Gatewayとデバイステレメトリの設定を確認（詳細はPalo Alto Networks社のWebサイトを参照）
2. GlobalProtect Gatewayとデバイステレメトリの両方が有効の場合、即座に以下の対応を実施。
   （特に、①は本日中に実施）
   ①　デバイステレメトリの無効化、および脅威ID 95187の有効化（脅威対策サブスクリプションを導入し

ている場合）

② 侵害有無の確認
Customer Support Portal （CSP）にてtechnical support file（TSF）をアップロードし既知のIoC（Indicators of Compromise）情報と突合する（詳細はPalo Alto Networks社のWebサイトを参照）。なお、パッチ適用やバージョンアップを行うとログが初期化されることがありますので、侵害有無確認はホットフィックスの適用前に実施すること。

③ ホットフィックスの適用（リリースされ次第）

以上

＜参考URL＞
Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性（CVE-2024-3400）に関する注意喚起（JPCERT/CC）
https://www.jpcert.or.jp/at/2024/at240009.html

CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect Gateway（Palo Alto Networks）
https://security.paloaltonetworks.com/CVE-2024-3400