

2024年4月17日

内閣官房 内閣サイバーセキュリティセンター
重要インフラグループ**Palo Alto Networks 製品の深刻な脆弱性 (CVE-2024-3400) について (注意喚起)
(第2報)**

2024年4月17日(水)(日本時間)、Palo Alto Networks は本脆弱性に関する情報を更新しました。これによれば、デバイステレメトリ機能の有効・無効にかかわらず本脆弱性は存在し、第1報にて緩和策とされた本機能の無効化は対処とならないことが明らかになっています。この脆弱性を悪用した攻撃の増加も確認されているため、対象ソフトウェアの最新バージョンへの更新を強く推奨します。引き続き、Palo Alto Networks からの情報を注視し適切に対応してください。本第2報は第1報(2024年4月15日付け Palo Alto Networks 製品の深刻な脆弱性 (CVE-2024-3400) について (注意喚起)) の内容を含みます。

1. 対象ソフトウェア

- ・ PAN-OS 11.1 11.1.2-h3 より前
- ・ PAN-OS 11.0 11.0.4-h1 より前
- ・ PAN-OS 10.2 10.2.9-h1 より前

2. 脆弱性悪用による影響等

対象ソフトウェアを使用しているネットワーク機器において、“GlobalProtect gateway”、“GlobalProtect portal” 又はその両方が設定されている場合、攻撃者によってルート権限で任意のコードを実行される恐れがあります。

3. 深刻度

ソフトウェアの開発元が深刻度「Critical」(5段階中、最高)に分類する脆弱性が含まれます。

4. 悪用

脆弱性を悪用した攻撃の増加が確認されています。

5. 対応

2024年4月15日12:00(日本時間)時点で本脆弱性が修正されたバージョンのソフトウェアが一部のバージョンについて公開されています。対象ソフトウェアの最新のバージョンへの更新を強く推奨します。

6. その他

参考に第1報を次ページに掲載します。

参考 URL

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

2024年4月15日

内閣官房 内閣サイバーセキュリティセンター
重要インフラグループ**Palo Alto Networks 製品の深刻な脆弱性 (CVE-2024-3400) について (注意喚起)**

1. 対象ソフトウェア

- ・ PAN-OS 11.1 11.1.2-h3 より前
- ・ PAN-OS 11.0 11.0.4-h1 より前
- ・ PAN-OS 10.2 10.2.9-h1 より前

2. 脆弱性悪用による影響等

対象ソフトウェアを使用しているネットワーク機器において、“GlobalProtect gateway”、“GlobalProtect portal” 又はその両方が設定されており、かつデバイステレメトリ機能が有効となっている場合、攻撃者によってルート権限で任意のコードを実行される恐れがあります。

3. 深刻度

ソフトウェアの開発元が深刻度「Critical」(5段階中、最高)に分類する脆弱性が含まれます。

4. 悪用

脆弱性を悪用した攻撃が確認されています。

5. 対応

2024年4月15日12:00(日本時間)時点で本脆弱性が修正されたバージョンのソフトウェアが一部のバージョンについて公開されています。対象ソフトウェアの最新のバージョンへの更新を強く推奨します。更新を直ちに実施できない場合は、緩和策(6.参照)の実施を検討してください。

6. その他

デバイステレメトリ機能を無効にしている場合、本脆弱性の影響は軽減されますが、ソフトウェアの健全性維持の観点からも、最新バージョンへの更新を強く推奨します。

参考 URL

- ・ CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect (Palo Alto Networks)
<https://security.paloaltonetworks.com/CVE-2024-3400>
- ・ 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>
- ・ Palo Alto Networks 製 PAN-OS の脆弱性対策について (CVE-2024-3400) (IPA)
<https://www.ipa.go.jp/security/security-alert/2024/alert20240415.html>