２０２３年１２月１８日

お客様各位

株式会社日立ソリューションズ
Palo Alto Networks 製品ユーザーサポート

BGP ソフトウェアのサービス拒否(DoS)の脆弱性(CVE-2023-38802)について(第 2 報)

平素は Palo Alto Networks 製品ユーザー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、BGP ソフトウェアのサービス拒否(DoS) の脆弱性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

   BGP を利用している場合に、攻撃者が無効な BGP アップデートを通じてネットワークセッションをリセットできる可能性がある脆弱性がございます。

2. 対象のお客様

   下記の表で影響を受けるバージョンをご利用されているお客様。

表 1 対象 OS バージョン

OS バージョン	影響を受ける	影響を受けない
Cloud NGFW	None	All
PAN-OS 11.0	< 11.0.3	≧ 11.0.3※1
PAN-OS 10.2	< 10.2.6	≧ 10.2.6※2
PAN-OS 10.1	< 10.1.11	≧ 10.1.11※2
PAN-OS 9.1	**< 9.1.16-h3**	**≧ 9.1.16-h3**※3
PAN-OS 9.0	**< 9.0.17-h4**	**≧ 9.0.17-h4**※4
PAN-OS 8.1	**< 8.1.26**	**≧ 8.1.26**※5
Prisma Access	最新のソフトウェアアップグレードを 2023/09/30(PST)以前に実施したお客様	2023/09/30(PST)以降にソフトウェアアップグレードを受け取った、または新しいソフトウェアを使用しているお客様

※1 2023/11/08 (JST) にリリース済みです。※2 2023/09/28 (JST) にリリース済みです。
※3 2023/10/04 (JST) にリリース済みです。※4 2023/12/05 (JST) にリリース済みです。
※5 2023/12/07 (JST) にリリース済みです。

3. 本脆弱性に該当する構成

本脆弱性は、BGP ルーティング機能が有効になっているデバイスとアプライアンスにのみ当てはまります。

PAN-OS ファイアウォールの Web UI から[NETWORK > 仮想ルーター or 論理ルーター > ルーター選択 > BGP] にて”有効化”のチェックが付いていた場合に当てはまります。

4. 回避策

本脆弱性の悪用を防ぐためには、攻撃者が発信した BGP アップデートと、PAN-OS および Prisma Access デバイスの間に、影響を受けない BGP ルーター（無効な BGP アップデートを伝播するのではなくドロップするように構成）を挿入します。これにより、無効な BGP アップデートが影響を受けるルーターに到達しなくなります。

5. 恒久対策

下記 OS バージョンへのアップグレードをご検討ください。

表 2 修正に対応している OS バージョン

対象 OS バージョン	修正 OS バージョン
Cloud NGFW	All
PAN-OS 11.0	≧ 11.0.3
PAN-OS 10.2	≧ 10.2.6
PAN-OS 10.1	≧ 10.1.11
PAN-OS 9.1	≧ **9.1.16-h3**
PAN-OS 9.0	**≧ 9.0.17-h4**
PAN-OS 8.1	**≧ 8.1.26**
Prisma Access	2023/09/30(PST)以降にソフトウェアアップグレードを受け取った、または新しいソフトウェアを使用しているお客様

※ 現在、PAN-OS 10.0 およびその他のサポート終了（EoL) PAN-OS バージョンでは、この問題の修正は予定されていません。

6. その他特記事項

本脆弱性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。

Security Advisories

CVE-2023-38802 PAN-OS: Denial-of-Service (DoS) Vulnerability in BGP Software

https://security.paloaltonetworks.com/CVE-2023-38802

以上