2025 年 07 月 15 日

お客様各位

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

【脆弱性】Junos OS 2025 年 7 月定期脆弱性報告における影響について

平素は Juniper 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 Juniper Networks 社より、深刻度の高い脆弱性として JSA100056 がアナウンスされましたので、下記の通りご連絡いたします。

敬具

記

1. 概要

RADIUS 認証における中間者攻撃の脆弱性(CVE-2024-3596)がアナウンスされています。

CVE：CVE-2024-3596

CVSS：9.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

Junos OS 製品における本脆弱性の影響は以下の通りです。

2. 対象のお客様

RADIUS を使用している、かつ以下のバージョンの Junos OS を使用している SRX / EX / QFX シリーズ製品

- Junos 21.4R3-S10 以前のすべてのバージョン
- Junos 22.2R3-S6 以前の 22.2 系
- Junos 22.4R3-S6 以前の 22.4 系
- Junos 23.2R2-S3 以前の 23.2 系
- Junos 23.4R2-S4 以前の 23.4 系
- Junos 24.2R2 以前の 24.2 系
- Junos 24.4R1-S2 以前の 24.4 系

3. 対策

本脆弱性は修正済みバージョンの Junos OS へアップグレードにより対策することができます。現在当社では、当該 OS のリリース準備を進めております。

なお、現在リリース済みの以下のバージョンで対策が可能です。

・SRX　: Junos 23.2R2-S4

・EX　: Junos 21.4R3-S11 (EX4300, EX4600 のみ)

その他の対策済み OS のリリース状況に関するお問い合わせについては、Juniper 製品 SRX 保守サービス仕様書、EX 保守サービス仕様書、QFX 保守サービス仕様書に記載の、「保守契約確認に必要な情報」をご確認の上、当社 Juniper Networks 製品ユーザーサポートまでご連絡ください。

4. 回避策

TLS を使用して RADIUS トラフィックを暗号化するための RADIUS over TLS (RADSEC) を有効にします。

コンフィグ : # set access radsec destination <ID> address x.x.x.x

5. Juniper Networks 社セキュリティアドバイザリ

Juniper Networks 社では、脆弱性情報を下記の Security Advisory ページで公開しています。最新の脆弱性情報は下記サイトをご覧いただき、適時ご利用環境の対策をいただきますようお願いいたします。

尚、同サイト記載以上の情報は開示されていません。記載内容の解釈および内容等については当社サポートではお答えいたしかねます。予めご了承ください。

Security Advisories

JSA100056

以上