2024 年 1 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 2024 年 1 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 JSA75729 が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。

敬具

記

1. 概要

SRX/EX 製品の J-Web 機能において以下の脆弱性が確認されています。

本脆弱性は SRX シリーズおよび EX シリーズの J-Web への領域外書き込みにより、認証されていないネットワークベースの攻撃者がサービス拒否(DoS)またはリモートコード実行(RCE)を引き起こし、デバイスでルート権限が取得され得ることから、メーカはクリティカルな脆弱性になると判断し、JSA75729 (CVE-2024-21591、CVSS Score: 9.8) をアナウンスしました。

2. 対象のお客様

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

- 20.4R3-S8 以前のすべてのバージョン
- 21.2R3-S6 以前の 21.2 系
- 21.3R3-S4 以前の 21.3 系
- 21.4R3-S4 以前の 21.4 系
- 22.1R3-S3 以前の 22.1 系
- 22.2R3-S2 以前の 22.2 系
- 22.3R3-S1 以前の 22.3 系
- 22.4R2-S1 以前の 22.4 系

3. 対策

本脆弱性は修正済みバージョンへの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。

尚、現在当社にて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 21.4R3-S5（加えて SRX1500 以上の機種は Junos 23.2R1-S1 でも対策可能）

・EX4100：Junos23.2R1-S1

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、または EX 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

以下のいずれかの方法で本脆弱性のリスクを軽減または回避することができます。

・J-Web を無効にする。

・信頼できるホストからのみのアクセスに制限する。

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

JSA75729

以上