2024 年 5 月 10 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 4 月定期脆弱性報告における影響について(第 2 報)

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 JSA79108 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。現在は CVSS スコア 6.4 (Medium)に引き下げられています。

敬具

記

1. 概要

Junos OS について、cURL ライブラリに含まれる以下の脆弱性がアナウンスされています。
4 月 23 日、26 日に JSA79108 に関する情報が更新され、いくつかの CVE の CVSS スコアが引き下げられました。

CVE	CVSS
CVE-2023-38545	6.4 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)
CVE-2023-38546	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
CVE-2023-23914	6.0 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)
CVE-2023-23915	4.4 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)
CVE-2020-8284	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
CVE-2020-8285	4.1 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N)
CVE-2020-8286	4.1 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N)

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 / QFX シリーズ製品
それぞれの CVE に対して影響を受ける Junos OS バージョンが公開されました。

CVE-2023-38545, CVE-2023-38546

・Junos 23.4R1-S1、23.4R2 より前のすべてのバージョン

CVE-2023-23914, CVE-2023-23915

・Junos 21.4R3-S5, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3 より前のすべてのバージョン

CVE-2020-8284, CVE-2020-8285, CVE-2020-8286

・Junos 21.2R1 より前のすべてのバージョン

3. 対策

本脆弱性は修正済みバージョンである、Junos 23.4R1-S1，23.4R2，24.2R1 およびそれ以降の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。

※5 月 10 日時点では 23.4R1-S1 のみ、メーカリリースされています。（SRX300 シリーズおよび QFX シリーズは除く）

現在当社では、当該 OS のリリース準備を進めております。

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

これらの問題に対する既知の回避策はありませんが、以下を実施することでリスクを軽減することができます。単一の実施では効果が薄いため、可能な限りすべて実施することを推奨します。

・信頼できるアクセスのみを許可する。
・シェルへのアクセスを最低限のユーザに制限する。
・UI サービスの利用を最低限にし、使用しない場合は無効にする。
・デバイスへのアクセスをコンソールサービスに制限し、必要な場合のみ SSH などの安全性の高いサービスを使用する。
・多要素認証を実装する。
・踏み台サーバを使用する場合、不正にアクセスされないネットワークセグメントに配置する。

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

JSA79108

以上