

2024年4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4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り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。

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。

CVE	CVSS
CVE-2023-38545	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/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	9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)
CVE-2023-23915	6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
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	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2020-8286	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/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

- ・ Junos 23.4R1-S1、23.4R2 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。

※4月15日時点では23.4R1-S1のみ、メーカー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。

### 5. Juniper Networks 社セキュリティアドバイザー

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ください、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