

2024年10月16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10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 [JSA88135](#) 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、Junos OS に含まれる nginx ソフトウェアに以下の脆弱性がアナウンスされています。

CVE	CVSS
CVE-2016-0742	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2016-0746	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2016-0747	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CVE-2016-1247	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2016-4450	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2017-7529	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVE-2017-20005	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2018-16845	6.1 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H)
CVE-2019-20372	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CVE-2021-3618	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
CVE-2021-23017	7.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L)
CVE-2022-41741	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-41742	7.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)
CVE-2023-44487	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

2. 対象のお客様

次の(1), (2) 両方を満たす SRX / EX / QFX シリーズ製品

(1) 以下のコンフィグのいずれかまたは両方を設定している。

- set system services webapi ~
- set system services extension-service request-response grpc ~

(2) 以下のバージョンの Junos OS を使用している

- Junos 21.4R3-S7 以前のすべてのバージョン
- Junos 22.2R3-S4 以前の 22.2 系
- Junos 22.3R3-S2 以前の 22.3 系
- Junos 22.4R3-S3 以前の 22.4 系
- Junos 23.2R2-S1 以前の 23.2 系
- Junos 23.4R2 以前の 23.4 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 : 21.4R3-S8, 23.4R2-S2 (SRX1600/2300 のみ)
- EX : 23.4R2-S2

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。

アクセスリストまたはファイアウォールフィルタを使用して、デバイスへのアクセスを信頼できる管理ネットワークまたはホストからのみに制限することで、リスクを軽減することができます。

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](#)

[JSA88135](#)

以上