2023 年 07 月 18 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 2023 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 JSA71653 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

- 概要

Junos OS に含まれるサードパーティ製ソフトウェアコンポーネントにおいて以下の脆弱性が確認されています。

CVE	CVSS
CVE-2022-31629	6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)
CVE-2022-31628	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
CVE-2022-31627	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-31626	8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-31625	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2021-21708	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2021-21707	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CVE-2021-21705	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CVE-2021-21704	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2021-21703	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2021-21702	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2020-7071	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

- 対象製品

Junos 23.2R1 より前のバージョンの Junos OS を使用している機器

- 対策

  本脆弱性は修正済みバージョンである Junos 23.2R1 以降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、当該バージョンのリリース準備を進めております。本バージョン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(または EX, MX, 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。

- 回避策

  本脆弱性は J-Web にて使用している PHP ソフトウェアに内在する脆弱性に起因して引き起こされます。したがって、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。

  - アクセスリストや firewall filter 機能を使用し、デバイスへのアクセスを信頼できるホストからのみに制限する。
  - J-Web へのアクセスを信頼できるネットワークのみに制限する。
  - J-Web を無効にする。

- 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実施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。記載内容の解釈また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

  ・JSA71653

以上