2023 年 11 月 30 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】SRX/EX 製品の J-Web 脆弱性における影響について(第 5 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 JSA72300 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

SRX/EX 製品の J-Web 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。

これらの脆弱性は、重要な機能に対する認証の欠落や、外部の攻撃者が環境変数を変更できる可能性があり、各個の脆弱性を組み合わせることで認証なしに外部から任意のコードを実行することが可能となるため、メーカはクリティカルな脆弱性になると判断し、JSA72300 (CVSS Score: 9.8) をアナウンスしました。

CVE	CVSS
CVE-2023-36844	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CVE-2023-36845	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2023-36846	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CVE-2023-36847	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
CVE-2023-36851	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

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
・21.1R1 以降のすべての 21.1 系
・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-S1 以前の 22.2 系
・22.3R2-S1 以前または 22.3R3 以前の 22.3 系
・22.4R2 以前の 22.4 系
・23.2R1

※ EX シリーズに関して影響範囲が修正され、SRX の影響範囲と同一になりました。

- 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、当該バージョン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にて、CVE-2023-36844, CVE-2023-36845, CVE-2023-36846, CVE-2023-36847 の対策が可能です。

・SRX：Junos 21.4R3-S5, 22.2R3-S2

その後の調査により、CVE-2023-36851 については、対策バージョンとして、不十分である可能性があり、現在メーカ確認中ですが、本脆弱性(JSA72300)は少なくとも上記 4 つの CVE に対する対策を行ったバージョンに変更することで、脅威に対するリスクを大幅に軽減できるとのメーカ見解です。

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 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。

・ 信頼できるホストからのみのアクセスに制限する。
・ 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

・JSA72300

以上

[改訂履歴]

改訂番号	発行年月	変更内容
初版	2023 年 8 月 22 日	新規発行
第 2 報	2023 年 9 月 1 日	「対象製品」項目の影響を受けるバージョンに Junos 21.1 系を追記
第 3 報	2023 年 9 月 13 日	メーカサイトの記載変更に伴い、以下のとおり改訂 ・「概要」項目に対象 CVE を追記 ・「対象製品」項目の影響を受けるバージョンを修正
第 4 報	2023 年 10 月 6 日	メーカサイトの記載変更に伴い、以下のとおり改訂 ・CVE-2023-36845 の CVSS スコアを 5.3 から 9.8 に改訂 ・EX シリーズの影響範囲を SRX シリーズと同一に修正 および以下を追記 ・当社でリリース済みの対策バージョンを記載
第 5 報	2023 年 11 月 30 日	メーカサイトの記載変更に伴い、対策バージョンについての案内に追記。