2024 年 1 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】Security Director Insights 2024 年 1 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 JSA75737 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

Security Director Insights に含まれるサードパーティライブラリにおいて以下の脆弱性が確認されています。

CVE	CVSS
CVE-2016-2183	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVE-2019-17571	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2020-9493	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-23302	8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-23305	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-23307	8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2023-26464	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2021-44228	10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVE-2021-44832	6.6 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

2. 対象のお客様

23.1R1 より前のバージョンの Security Director Insights を使用しているお客様

3. 対策

本脆弱性は修正済みバージョンである 23.1R1 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 OS のリリース準備を進めております。本 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 Junos Space 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

以下の方法で本脆弱性のリスクを軽減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。

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

JSA75737

以上