

2023年1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 Space Security Director 2023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 JSA70185 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 Space に含まれるサードパーティ製ソフトウェアにおいて以下の脆弱性が確認されています。

CVE	CVSS
CVE-2022-29154	7.4(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H)
CVE-2022-2526	9.8(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-21541	5.9(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)
CVE-2022-34169	7.5(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CVE-2022-21540	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CVE-2022-21624	3.7(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
CVE-2022-21626	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CVE-2022-21628	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CVE-2022-21619	3.7(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
CVE-2007-2285	7.8 (AV:N/AC:L/Au:N/C:C/I:N/A:N)
CVE-2018-8046	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2020-26137	6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
CVE-2021-3177	9.8(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2020-26116	7.2 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N)
CVE-2022-1729	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-32250	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2022-1271	8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

2. 対象のお客様

22.3R1 より前のバージョンの Junos Space 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 22.3R1 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. 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](#)

・ [JSA70185](#)

以上