ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans Juniper Secure Analytics
Numéro de Référence	47912006/24
Date de Publication	20 Juin 2024
Risque	Important
Impact	Important

Systèmes affectés

- Juniper Secure Analytics versions antérieures à 7.5.0 UP8 IF03

Identificateurs externes

- CVE-2001-1267 CVE-2007-4559 CVE-2011-4969 CVE-2012-6708 CVE-2014-3146 CVE-2015-9251 CVE-2017-7500 CVE-2017-7501 CVE-2018-19787 CVE-2019-13224 CVE-2019-13631 CVE-2019-15505 CVE-2019-16163 CVE-2019-19012 CVE-2019-19203 CVE-2019-19204 CVE-2019-8675 CVE-2019-8696 CVE-2020-10001 CVE-2020-25656 CVE-2020-27783 CVE-2020-28241 CVE-2020-3898 CVE-2020-7656 CVE-2021-33631 CVE-2021-35937 CVE-2021-35938 CVE-2021-35939 CVE-2021-3753 CVE-2021-41043 CVE-2021-4204 CVE-2021-43618 CVE-2021-43818 CVE-2021-43975 CVE-2022-0500 CVE-2022-2127 CVE-2022-23222 CVE-2022-26377 CVE-2022-26691 CVE-2022-28388 CVE-2022-3094 CVE-2022-3545 CVE-2022-3565 CVE-2022-3594 CVE-2022-3640 CVE-2022-36402 CVE-2022-38096 CVE-2022-38457 CVE-2022-40133 CVE-2022-40982 CVE-2022-41858 CVE-2022-42895 CVE-2022-45061 CVE-2022-45869 CVE-2022-45884 CVE-2022-45887 CVE-2022-45919 CVE-2022-45934 CVE-2022-46329 CVE-2022-4744 CVE-2022-48560 CVE-2022-48564 CVE-2022-48624 CVE-2023-0458 CVE-2023-0590 CVE-2023-0597 CVE-2023-1073 CVE-2023-1074 CVE-2023-1075 CVE-2023-1079 CVE-2023-1118 CVE-2023-1192 CVE-2023-1206 CVE-2023-1252 CVE-2023-1382 CVE-2023-1513 CVE-2023-1786 CVE-2023-1838 CVE-2023-1855 CVE-2023-1989 CVE-2023-1998 CVE-2023-20569 CVE-2023-2162 CVE-2023-2163 CVE-2023-2166 CVE-2023-2176 CVE-2023-22067 CVE-2023-22081 CVE-2023-23455 CVE-2023-24023 CVE-2023-25012 CVE-2023-2513 CVE-2023-25775 CVE-2023-26545 CVE-2023-26604 CVE-2023-27043 CVE-2023-2828 CVE-2023-28322 CVE-2023-28328 CVE-2023-28464 CVE-2023-28486 CVE-2023-28487 CVE-2023-28772 CVE-2023-30456 CVE-2023-31083 CVE-2023-31084 CVE-2023-3138 CVE-2023-3141 CVE-2023-31436 CVE-2023-3161 CVE-2023-3212 CVE-2023-32324 CVE-2023-32360 CVE-2023-3268 CVE-2023-33203

CVE-2023-3341 CVE-2023-33951 CVE-2023-33952 CVE-2023-34241 CVE-2023-34966 CVE-2023-34967 CVE-2023-34968 CVE-2023-3567 CVE-2023-35823 CVE-2023-35824 CVE-2023-3609 CVE-2023-3611 CVE-2023-37453 CVE-2023-3758 CVE-2023-3772 CVE-2023-3812 CVE-2023-38409 CVE-2023-38546 CVE-2023-39189 CVE-2023-39192 CVE-2023-39193 CVE-2023-39194 CVE-2023-39198 CVE-2023-39615 CVE-2023-40283 CVE-2023-40546 CVE-2023-40547 CVE-2023-40548 CVE-2023-40549 CVE-2023-40550 CVE-2023-40551 CVE-2023-4091 CVE-2023-4128 CVE-2023-4132 CVE-2023-4133 CVE-2023-4155 CVE-2023-4206 CVE-2023-4207 CVE-2023-4208 CVE-2023-4244 CVE-2023-42465 CVE-2023-42669 CVE-2023-42753 CVE-2023-42754 CVE-2023-42755 CVE-2023-43804 CVE-2023-4408 CVE-2023-45803 CVE-2023-45862 CVE-2023-45863 CVE-2023-45871 CVE-2023-46218 CVE-2023-4622 CVE-2023-4623 CVE-2023-46813 CVE-2023-4732 CVE-2023-48795 CVE-2023-4921 CVE-2023-50387 CVE-2023-50868 CVE-2023-50960 CVE-2023-50961 CVE-2023-51042 CVE-2023-51043 CVE-2023-51385 CVE-2023-51779 CVE-2023-5178 CVE-2023-51780 CVE-2023-52340 CVE-2023-52425 CVE-2023-52434 CVE-2023-52448 CVE-2023-52489 CVE-2023-52574 CVE-2023-52580 CVE-2023-52581 CVE-2023-52620 CVE-2023-5388 CVE-2023-5633 CVE-2023-5676 CVE-2023-5717 CVE-2023-5981 CVE-2023-6121 CVE-2023-6135 CVE-2023-6176 CVE-2023-6356 CVE-2023-6535 CVE-2023-6536 CVE-2023-6546 CVE-2023-6606 CVE-2023-6610 CVE-2023-6622 CVE-2023-6817 CVE-2023-6915 CVE-2023-6931 CVE-2023-6932 CVE-2023-7192 CVE-2024-0553 CVE-2024-0565 CVE-2024-0646 CVE-2024-0841 CVE-2024-1086 CVE-2024-1488 CVE-2024-22243 CVE-2024-22259 CVE-2024-22262 CVE-2024-25742 CVE-2024-25743 CVE-2024-26602 CVE-2024-26609 CVE-2024-26671 CVE-2024-27269 CVE-2024-28784

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les versions susmentionnées de Juniper Secure Analytics. L'exploitation de ces failles peut permettre à un attaquant de porter atteinte à la confidentialité des données, de contourner la politique de sécurité et d'exécuter du code arbitraire à distance, de réussir une élévation de privilèges et de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité Juniper du 19 juin 2024**.**

Risque

- Exécution de code arbitraire à distance
- Contournement de la politique de sécurité
- Atteinte à la confidentialité des données
- Elévation de privilèges
- Déni de service

Annexe

Bulletin de sécurité Juniper du 19 juin 2024**:**

- https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP8-IF03