DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 26-07-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans IBM QRadar
Réference	1193
Date de Publication	2024-07-26
Sévérité	Elevé

IMPACT :

- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Exécution de code arbitraire à distance
- Injection de code indirecte à distance (XSS)
- Élévation de privilèges

SYSTÉME AFFECTÉ :

- QRadar Data Synchronization App versions antérieures à 3.2.0
- QRadar Network Packet Capture versions 7.5.0 antérieures à 7.5.0 Update Package 8
- QRadar Pulse App versions antérieures à 2.2.14

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans IBM QRadar. Certaines de ces vulnérabilités permettent à un attaquant d'exécuter du code arbitraire à distance, d'élever ses privilèges ou de provoquer un déni de service à distance.

SOLUTION :

Mettre à jour IBM QRadar.(se réfère à la documentation)

DOCUMENTATION :

- Bulletin de sécurité IBM 7160858 du 22 juillet 2024

https://www.ibm.com/support/pages/node/7160858

- Bulletin de sécurité IBM 7160961 du 23 juillet 2024

https://www.ibm.com/support/pages/node/7160961

- Bulletin de sécurité IBM 7161462 du 24 juillet 2024

https://www.ibm.com/support/pages/node/7161462

- CVE-2016-10538

https://www.cve.org/CVERecord?id=CVE-2016-10538

- CVE-2016-10540

https://www.cve.org/CVERecord?id=CVE-2016-10540

- CVE-2018-16487

https://www.cve.org/CVERecord?id=CVE-2018-16487

- CVE-2018-3721

https://www.cve.org/CVERecord?id=CVE-2018-3721

- CVE-2020-28477

https://www.cve.org/CVERecord?id=CVE-2020-28477

- CVE-2021-23364

https://www.cve.org/CVERecord?id=CVE-2021-23364

- CVE-2021-23436

https://www.cve.org/CVERecord?id=CVE-2021-23436

- CVE-2021-24033

https://www.cve.org/CVERecord?id=CVE-2021-24033

- CVE-2021-3757

https://www.cve.org/CVERecord?id=CVE-2021-3757

- CVE-2021-42740

https://www.cve.org/CVERecord?id=CVE-2021-42740

- CVE-2021-43138

https://www.cve.org/CVERecord?id=CVE-2021-43138

- CVE-2022-25881

https://www.cve.org/CVERecord?id=CVE-2022-25881

- CVE-2022-25883

https://www.cve.org/CVERecord?id=CVE-2022-25883

- CVE-2022-3517

https://www.cve.org/CVERecord?id=CVE-2022-3517

- CVE-2022-37601

https://www.cve.org/CVERecord?id=CVE-2022-37601

- CVE-2022-37603

https://www.cve.org/CVERecord?id=CVE-2022-37603

- CVE-2022-43441

https://www.cve.org/CVERecord?id=CVE-2022-43441

- CVE-2023-0361

https://www.cve.org/CVERecord?id=CVE-2023-0361

- CVE-2023-0842

https://www.cve.org/CVERecord?id=CVE-2023-0842

- CVE-2023-32233

https://www.cve.org/CVERecord?id=CVE-2023-32233

- CVE-2023-3341

https://www.cve.org/CVERecord?id=CVE-2023-3341

- CVE-2023-3446

https://www.cve.org/CVERecord?id=CVE-2023-3446

- CVE-2023-35001

https://www.cve.org/CVERecord?id=CVE-2023-35001

- CVE-2023-3609

https://www.cve.org/CVERecord?id=CVE-2023-3609

- CVE-2023-36632

https://www.cve.org/CVERecord?id=CVE-2023-36632

- CVE-2023-3817

https://www.cve.org/CVERecord?id=CVE-2023-3817

- CVE-2023-38546

https://www.cve.org/CVERecord?id=CVE-2023-38546

- CVE-2023-39615

https://www.cve.org/CVERecord?id=CVE-2023-39615

- CVE-2023-40217

https://www.cve.org/CVERecord?id=CVE-2023-40217

- CVE-2023-42282

https://www.cve.org/CVERecord?id=CVE-2023-42282

- CVE-2023-45133

https://www.cve.org/CVERecord?id=CVE-2023-45133

- CVE-2023-4806

https://www.cve.org/CVERecord?id=CVE-2023-4806

- CVE-2023-4813

https://www.cve.org/CVERecord?id=CVE-2023-4813

- CVE-2023-48795

https://www.cve.org/CVERecord?id=CVE-2023-48795

- CVE-2023-51385

https://www.cve.org/CVERecord?id=CVE-2023-51385

- CVE-2023-5156

https://www.cve.org/CVERecord?id=CVE-2023-5156

- CVE-2023-5678

https://www.cve.org/CVERecord?id=CVE-2023-5678

- CVE-2023-5981

https://www.cve.org/CVERecord?id=CVE-2023-5981

- CVE-2023-6129

https://www.cve.org/CVERecord?id=CVE-2023-6129

- CVE-2024-0553

https://www.cve.org/CVERecord?id=CVE-2024-0553

- CVE-2024-0567

https://www.cve.org/CVERecord?id=CVE-2024-0567

- CVE-2024-27088

https://www.cve.org/CVERecord?id=CVE-2024-27088

- CVE-2024-27982

https://www.cve.org/CVERecord?id=CVE-2024-27982

- CVE-2024-27983

https://www.cve.org/CVERecord?id=CVE-2024-27983

- CVE-2024-28834

https://www.cve.org/CVERecord?id=CVE-2024-28834

- CVE-2024-28835

https://www.cve.org/CVERecord?id=CVE-2024-28835

- CVE-2024-28863

https://www.cve.org/CVERecord?id=CVE-2024-28863

- CVE-2024-29041

https://www.cve.org/CVERecord?id=CVE-2024-29041

- CVE-2024-29415

https://www.cve.org/CVERecord?id=CVE-2024-29415

- CVE-2024-2961

https://www.cve.org/CVERecord?id=CVE-2024-2961

- CVE-2024-31905

https://www.cve.org/CVERecord?id=CVE-2024-31905

- CVE-2024-33599

https://www.cve.org/CVERecord?id=CVE-2024-33599

- CVE-2024-33600

https://www.cve.org/CVERecord?id=CVE-2024-33600

- CVE-2024-33601

https://www.cve.org/CVERecord?id=CVE-2024-33601

- CVE-2024-33602

https://www.cve.org/CVERecord?id=CVE-2024-33602

- CVE-2024-4067

https://www.cve.org/CVERecord?id=CVE-2024-4067

- CVE-2024-4068

https://www.cve.org/CVERecord?id=CVE-2024-4068