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

Autorité Nationale de Cybersécurité

Djibouti le, 06-05-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilité dans les produit IBM
Réference	1137
Date de Publication	2024-05-06
Sévérité	Critique

IMPACT :

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

SYSTÉME AFFECTÉ :

- QRadar Assistant versions antérieures à 3.7.0
- QRadar SIEM sur Azure Marketplace versions antérieures à 7.3.x postérieures à 7.3.3 et antérieures à 7.5.0 avec le paquet OMI installé
- Cognos Analytics versions 12.0.x antérieures à 12.0.3
- Cognos Analytics versions 11.2.x FP2 antérieures à 11.2.4 FP3
- WebSphere eXtreme Scale versions 8.6.1.x antérieures à 8.6.1.6 sans le correctif de sécurité PH61029
- IBM Cloud Pak for Security versions 1.10.x.x antérieures à 1.10.21.0
- QRadar Suite Software versions 1.10.x.x antérieures à 1.10.21.0

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes dans les produits IBM susmentionné.

Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un déni de service à distance.

SOLUTION :

Mettre à jour les produits IBM. (se réfère à la documentation)

DOCUMENTATION :

- Bulletin de sécurité IBM 7149736 du 29/05/2024
  https://www.ibm.com/support/pages/node/7149736
- Bulletin de sécurité IBM 7149967 du 01/05/2024
  https://www.ibm.com/support/pages/node/7149967
- Bulletin de sécurité IBM 7149874 du 01/05/2024
  https://www.ibm.com/support/pages/node/7149874
- Bulletin de sécurité IBM 7150045 du 01/05/2024
  https://www.ibm.com/support/pages/node/7150045
- Bulletin de sécurité IBM 7150150 du 03/05/2024
  https://www.ibm.com/support/pages/node/7150150
- CVE-2015-3627
  https://www.cve.org/CVERecord?id=CVE-2015-3627
- CVE-2016-10516
  https://www.cve.org/CVERecord?id=CVE-2016-10516
- CVE-2016-10745
  https://www.cve.org/CVERecord?id=CVE-2016-10745
- CVE-2018-1000656
  https://www.cve.org/CVERecord?id=CVE-2018-1000656
- CVE-2018-18074
  https://www.cve.org/CVERecord?id=CVE-2018-18074
- Référence CVE CVE-2019-1010083
  https://www.cve.org/CVERecord?id=CVE-2019-1010083
- Référence CVE CVE-2019-14322
  https://www.cve.org/CVERecord?id=CVE-2019-14322
- CVE-2020-15366
  https://www.cve.org/CVERecord?id=CVE-2020-15366
- CVE-2020-25032
  https://www.cve.org/CVERecord?id=CVE-2020-25032
- CVE-2020-28493
  https://www.cve.org/CVERecord?id=CVE-2020-28493
- CVE-2021-28363
  https://www.cve.org/CVERecord?id=CVE-2021-28363
- CVE-2021-30465
  https://www.cve.org/CVERecord?id=CVE-2021-30465

- CVE-2021-43565
  https://www.cve.org/CVERecord?id=CVE-2021-43565
- CVE-2021-43784
  https://www.cve.org/CVERecord?id=CVE-2021-43784
- CVE-2021-45958
  https://www.cve.org/CVERecord?id=CVE-2021-45958
- CVE-2022-23539
  https://www.cve.org/CVERecord?id=CVE-2022-23539
- CVE-2022-23540
  https://www.cve.org/CVERecord?id=CVE-2022-23540
- CVE-2022-23541
  https://www.cve.org/CVERecord?id=CVE-2022-23541
- CVE-2022-29162
  https://www.cve.org/CVERecord?id=CVE-2022-29162
- CVE-2022-31116
  https://www.cve.org/CVERecord?id=CVE-2022-31116
- CVE-2022-31117
  https://www.cve.org/CVERecord?id=CVE-2022-31117
- CVE-2022-40897
  https://www.cve.org/CVERecord?id=CVE-2022-40897
- CVE-2023-23934
  https://www.cve.org/CVERecord?id=CVE-2023-23934
- CVE-2023-25577
  https://www.cve.org/CVERecord?id=CVE-2023-25577
- CVE-2023-25809
  https://www.cve.org/CVERecord?id=CVE-2023-25809
- CVE-2023-26159
  https://www.cve.org/CVERecord?id=CVE-2023-26159
- CVE-2023-27561
  https://www.cve.org/CVERecord?id=CVE-2023-27561
- CVE-2023-28642
  https://www.cve.org/CVERecord?id=CVE-2023-28642
- CVE-2023-28840
  https://www.cve.org/CVERecord?id=CVE-2023-28840
- CVE-2023-28841
  https://www.cve.org/CVERecord?id=CVE-2023-28841
- CVE-2023-28842
  https://www.cve.org/CVERecord?id=CVE-2023-28842
- CVE-2023-30861
  https://www.cve.org/CVERecord?id=CVE-2023-30861
- CVE-2023-31484
  https://www.cve.org/CVERecord?id=CVE-2023-31484
- CVE-2023-32681
  https://www.cve.org/CVERecord?id=CVE-2023-32681
- CVE-2023-34462
  https://www.cve.org/CVERecord?id=CVE-2023-34462
- CVE-2023-44270
  https://www.cve.org/CVERecord?id=CVE-2023-44270
- CVE-2023-44487
  https://www.cve.org/CVERecord?id=CVE-2023-44487

- CVE-2023-44981
  https://www.cve.org/CVERecord?id=CVE-2023-44981
- CVE-2023-45857
  https://www.cve.org/CVERecord?id=CVE-2023-45857
- CVE-2023-46136
  https://www.cve.org/CVERecord?id=CVE-2023-46136
- CVE-2023-5072
  https://www.cve.org/CVERecord?id=CVE-2023-5072
- CVE-2024-1135
  https://www.cve.org/CVERecord?id=CVE-2024-1135
- CVE-2024-21334
  https://www.cve.org/CVERecord?id=CVE-2024-21334
- CVE-2024-21501
  https://www.cve.org/CVERecord?id=CVE-2024-21501
- CVE-2024-21503
  https://www.cve.org/CVERecord?id=CVE-2024-21503
- CVE-2024-22195
  https://www.cve.org/CVERecord?id=CVE-2024-22195
- CVE-2024-24758
  https://www.cve.org/CVERecord?id=CVE-2024-24758
- CVE-2024-25047
  https://www.cve.org/CVERecord?id=CVE-2024-25047
- CVE-2024-27088
  https://www.cve.org/CVERecord?id=CVE-2024-27088
- CVE-2024-28102
  https://www.cve.org/CVERecord?id=CVE-2024-28102
- CVE-2024-28849
  https://www.cve.org/CVERecord?id=CVE-2024-28849
- CVE-2024-29131
  https://www.cve.org/CVERecord?id=CVE-2024-29131
- CVE-2024-29133

https://www.cve.org/CVERecord?id=CVE-2024-29133