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

Autorité Nationale de Cybersécurité

Djibouti le, 21-01-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilité dans les produit IBM
Réference	1093
Date de Publication	2024-01-20
Sévérité	Critique

IMPACT :

- Non spécifié par l'éditeur
- 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
- Injection de code indirecte à distance (XSS)

SYSTÉME AFFECTÉ :

- IBM Sterling Transformation Extender versions 10.1.0, 10.1.1, 10.1.2 et 11.0.0 sans le correctif de sécurité PH58718
- IBM QRadar SIEM versions 7.5. à 7.5.0 UP7 sans le correctif de sécurité 7.5.0 UP7 IF04
- IBM Sterling Connect Direct pour Microsoft Windows versions 6.0.0.x antérieures à 6.0.0.4_iFix083
- IBM Sterling Connect Direct pour Microsoft Windows versions 6.1.0.x antérieures à 6.1.0.2_iFix079
- IBM Sterling Connect Direct pour Microsoft Windows versions 6.2.0.x antérieures à 6.2.0.6_iFix006
- IBM Sterling Connect Direct pour Microsoft Windows versions 6.3.0.x antérieures à 6.3.0.2_iFix005

DÉSCRIPTION :

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

Ces vulnérabilités permettent à un attaquant distant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et un déni de service à distance.

SOLUTION :

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

DOCUMENTATION :

- Bulletin de sécurité IBM 7108659 du 17-01-2024
  https://www.ibm.com/support/pages/node/7108659
- CVE-2022-40152
  https://www.cve.org/CVERecord?id=CVE-2022-40152
- CVE-2023-21930
  https://www.cve.org/CVERecord?id=CVE-2023-21930
- CVE-2023-21937
  https://www.cve.org/CVERecord?id=CVE-2023-21937
- CVE-2023-21938
  https://www.cve.org/CVERecord?id=CVE-2023-21938
- CVE-2023-21939
  https://www.cve.org/CVERecord?id=CVE-2023-21939
- CVE-2023-21954
  https://www.cve.org/CVERecord?id=CVE-2023-21954
- CVE-2023-21967
  https://www.cve.org/CVERecord?id=CVE-2023-21967
- CVE-2023-21968
  https://www.cve.org/CVERecord?id=CVE-2023-21968
- CVE-2023-2597
  https://www.cve.org/CVERecord?id=CVE-2023-2597
- CVE-2023-34058
  https://www.cve.org/CVERecord?id=CVE-2023-34058
- CVE-2023-34059
  https://www.cve.org/CVERecord?id=CVE-2023-34059
- CVE-2023-36478
  https://www.cve.org/CVERecord?id=CVE-2023-36478
- CVE-2023-36479
  https://www.cve.org/CVERecord?id=CVE-2023-36479
- CVE-2023-40167
  https://www.cve.org/CVERecord?id=CVE-2023-40167
- CVE-2023-40217
  https://www.cve.org/CVERecord?id=CVE-2023-40217
- CVE-2023-41900
  https://www.cve.org/CVERecord?id=CVE-2023-41900
- CVE-2023-44487
  https://www.cve.org/CVERecord?id=CVE-2023-44487
- CVE-2023-50164
  https://www.cve.org/CVERecord?id=CVE-2023-50164
- CVE-2023-50950
  https://www.cve.org/CVERecord?id=CVE-2023-50950