

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 18-11-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits IBM
Référence	1276
Date de Publication	2024-11-18
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

SYSTÈME AFFECTÉ :

- IBM Sterling B2B Integrator versions 6.2x antérieures à 6.2.0.3
- IBM Sterling B2B Integrator versions 6.x antérieures à 6.1.2.6
- IBM Sterling Connect:Direct Web Services versions 6.1.x antérieures à 6.1.0.26
- IBM Sterling Connect:Direct Web Services versions 6.2.x antérieures à 6.2.0.25
- IBM Sterling Connect:Direct Web Services versions 6.3.x antérieures à 6.3.0.10
- IBM Sterling Control Center versions 6.2.1.x antérieures à 6.2.1.0 iFix14
- IBM Sterling Control Center versions 6.3.1.x antérieures à 6.3.1.0 iFix03
- IBM Sterling Secure Proxy versions 6.0.x antérieures à 6.0.3.1
- IBM Sterling Secure Proxy versions 6.1.x antérieures à 6.1.0.1
- IBM Sterling Transformation Extender versions 10.1.0.x antérieures à 10.1.0.2 avec les derniers correctifs de sécurité
- IBM Sterling Transformation Extender versions 10.1.1.x antérieures à 10.1.1.1 avec les derniers correctifs de sécurité
- IBM Sterling Transformation Extender versions 10.1.2.x antérieures à 10.1.2.1 avec les derniers correctifs de sécurité
- IBM Sterling Transformation Extender versions 11.x antérieures à 11.0.0.0 avec les derniers correctifs de sécurité
- QRadar WinCollect Agent versions 10.x antérieures à 10.1.13
- WebSphere eXtreme Scale versions 8.6.x antérieures à 8.6.1.6 avec les derniers correctifs de sécurité

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans les produits IBM, permettant à un attaquant d'exécuter du code arbitraire à distance, de réaliser une élévation de privilèges et de provoquer un déni de service à distance.

SOLUTION :

Consultez le bulletin de sécurité de l'éditeur pour obtenir les correctifs nécessaires (voir section Documentation).

DOCUMENTATION :

- Bulletin de sécurité IBM 7175229 du 08 novembre 2024

<https://www.ibm.com/support/pages/node/7175229>

- Bulletin de sécurité IBM 7175724 du 12 novembre 2024

<https://www.ibm.com/support/pages/node/7175724>

- Bulletin de sécurité IBM 7175729 du 12 novembre 2024

<https://www.ibm.com/support/pages/node/7175729>

- Bulletin de sécurité IBM 7175883 du 13 novembre 2024

<https://www.ibm.com/support/pages/node/7175883>

- Bulletin de sécurité IBM 7176022 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176022>

- Bulletin de sécurité IBM 7176037 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176037>

- Bulletin de sécurité IBM 7176039 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176039>

- Bulletin de sécurité IBM 7176043 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176043>

- Bulletin de sécurité IBM 7176045 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176045>

- Bulletin de sécurité IBM 7176055 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176055>

- Bulletin de sécurité IBM 7176063 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176063>

- Bulletin de sécurité IBM 7176066 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176066>

- Bulletin de sécurité IBM 7176069 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176069>

- Bulletin de sécurité IBM 7176189 du 14 novembre 2024

<https://www.ibm.com/support/pages/node/7176189>

- Référence CVE CVE-2018-11784

<https://www.cve.org/CVERecord?id=CVE-2018-11784>

- Référence CVE CVE-2021-32808

<https://www.cve.org/CVERecord?id=CVE-2021-32808>

- Référence CVE CVE-2021-32809

<https://www.cve.org/CVERecord?id=CVE-2021-32809>

- Référence CVE CVE-2021-37695

<https://www.cve.org/CVERecord?id=CVE-2021-37695>

- Référence CVE CVE-2021-41164

<https://www.cve.org/CVERecord?id=CVE-2021-41164>

- Référence CVE CVE-2021-41165

<https://www.cve.org/CVERecord?id=CVE-2021-41165>

- Référence CVE CVE-2022-24728

<https://www.cve.org/CVERecord?id=CVE-2022-24728>

- Référence CVE CVE-2022-24729

<https://www.cve.org/CVERecord?id=CVE-2022-24729>

- Référence CVE CVE-2022-45688

<https://www.cve.org/CVERecord?id=CVE-2022-45688>

- Référence CVE CVE-2023-28439

<https://www.cve.org/CVERecord?id=CVE-2023-28439>

- Référence CVE CVE-2023-31582

<https://www.cve.org/CVERecord?id=CVE-2023-31582>

- Référence CVE CVE-2023-4771

<https://www.cve.org/CVERecord?id=CVE-2023-4771>

- Référence CVE CVE-2023-50314

<https://www.cve.org/CVERecord?id=CVE-2023-50314>

- Référence CVE CVE-2023-5072

<https://www.cve.org/CVERecord?id=CVE-2023-5072>

- Référence CVE CVE-2023-51441

<https://www.cve.org/CVERecord?id=CVE-2023-51441>

- Référence CVE CVE-2023-51775

<https://www.cve.org/CVERecord?id=CVE-2023-51775>

- Référence CVE CVE-2024-21131

<https://www.cve.org/CVERecord?id=CVE-2024-21131>

- Référence CVE CVE-2024-21138

<https://www.cve.org/CVERecord?id=CVE-2024-21138>

- Référence CVE CVE-2024-21140

<https://www.cve.org/CVERecord?id=CVE-2024-21140>

- Référence CVE CVE-2024-21144

<https://www.cve.org/CVERecord?id=CVE-2024-21144>

- Référence CVE CVE-2024-21145

<https://www.cve.org/CVERecord?id=CVE-2024-21145>

- Référence CVE CVE-2024-21147

<https://www.cve.org/CVERecord?id=CVE-2024-21147>

- Référence CVE CVE-2024-22329

<https://www.cve.org/CVERecord?id=CVE-2024-22329>

- Référence CVE CVE-2024-22353

<https://www.cve.org/CVERecord?id=CVE-2024-22353>

- Référence CVE CVE-2024-22354

<https://www.cve.org/CVERecord?id=CVE-2024-22354>

- Référence CVE CVE-2024-24815

<https://www.cve.org/CVERecord?id=CVE-2024-24815>

- Référence CVE CVE-2024-24816

<https://www.cve.org/CVERecord?id=CVE-2024-24816>

- Référence CVE CVE-2024-25015

<https://www.cve.org/CVERecord?id=CVE-2024-25015>

- Référence CVE CVE-2024-25026

<https://www.cve.org/CVERecord?id=CVE-2024-25026>

- Référence CVE CVE-2024-25048

<https://www.cve.org/CVERecord?id=CVE-2024-25048>

- Référence CVE CVE-2024-27267

<https://www.cve.org/CVERecord?id=CVE-2024-27267>

- Référence CVE CVE-2024-27268

<https://www.cve.org/CVERecord?id=CVE-2024-27268>

- Référence CVE CVE-2024-27270

<https://www.cve.org/CVERecord?id=CVE-2024-27270>

- Référence CVE CVE-2024-29857

<https://www.cve.org/CVERecord?id=CVE-2024-29857>

- Référence CVE CVE-2024-30171

<https://www.cve.org/CVERecord?id=CVE-2024-30171>

- Référence CVE CVE-2024-30172

<https://www.cve.org/CVERecord?id=CVE-2024-30172>

- Référence CVE CVE-2024-41783

<https://www.cve.org/CVERecord?id=CVE-2024-41783>

- Référence CVE CVE-2024-45296

<https://www.cve.org/CVERecord?id=CVE-2024-45296>

- Référence CVE CVE-2024-51462

<https://www.cve.org/CVERecord?id=CVE-2024-51462>

- Référence CVE CVE-2024-7348

<https://www.cve.org/CVERecord?id=CVE-2024-7348>

- Référence CVE CVE-2024-8096

<https://www.cve.org/CVERecord?id=CVE-2024-8096>

- Référence CVE CVE-2024-9681

<https://www.cve.org/CVERecord?id=CVE-2024-9681>