

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 29-06-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilité dans les produit IBM
Référence	1172
Date de Publication	2024-06-28
Sévérité	Critique

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
- Élévation de privilèges
- Injection de code indirecte à distance (XSS)

SYSTÈME AFFECTÉ :

- IBM Cognos Analytics versions 11.2.x antérieures à 11.2.4 FP4
- IBM Cognos Analytics versions 12.x antérieures à 12.0.3 IF1
- IBM Cognos Dashboards sur Cloud Pak for Data versions antérieures à 5.0
- IBM WebSphere Hybrid Edition version 5.1 sans le dernier correctif de sécurité (APAR PH61504) pour IBM WebSphere Application Server
- IBM WebSphere Remote Server versions 9.1, 9.0 et 8.5 sans le dernier correctif de sécurité (APAR PH61504) pour IBM WebSphere Application Server
- WebSphere Service Registry and Repository version 8.5 sans le dernier correctif de sécurité (APAR PH61504) pour IBM WebSphere Application Server

DÉSCRIPTION :

De multiples vulnérabilités ont été découvertes dans les produits IBM. 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 7158537 du 24 juin 2024

<https://www.ibm.com/support/pages/node/7158537>

- Bulletin de sécurité IBM 7158539 du 24 juin 2024

<https://www.ibm.com/support/pages/node/7158539>

- Bulletin de sécurité IBM 7158652 du 25 juin 2024

<https://www.ibm.com/support/pages/node/7158652>

- Bulletin de sécurité IBM 7158762 du 26 juin 2024

<https://www.ibm.com/support/pages/node/7158762>

- Bulletin de sécurité IBM 7156941 du 27 juin 2024

<https://www.ibm.com/support/pages/node/7156941>

- Bulletin de sécurité IBM 7157712 du 27 juin 2024

<https://www.ibm.com/support/pages/node/7157712>

- CVE-2010-4756

<https://www.cve.org/CVERecord?id=CVE-2010-4756>

- CVE-2017-20162

<https://www.cve.org/CVERecord?id=CVE-2017-20162>

- CVE-2017-20189

<https://www.cve.org/CVERecord?id=CVE-2017-20189>

- CVE-2018-9466

<https://www.cve.org/CVERecord?id=CVE-2018-9466>

- CVE-2019-0231

<https://www.cve.org/CVERecord?id=CVE-2019-0231>

- CVE-2021-20086

<https://www.cve.org/CVERecord?id=CVE-2021-20086>

- CVE-2021-23358

<https://www.cve.org/CVERecord?id=CVE-2021-23358>

- CVE-2021-3377

<https://www.cve.org/CVERecord?id=CVE-2021-3377>

- CVE-2021-36770

<https://www.cve.org/CVERecord?id=CVE-2021-36770>

- CVE-2021-41973

<https://www.cve.org/CVERecord?id=CVE-2021-41973>

- CVE-2022-24785

<https://www.cve.org/CVERecord?id=CVE-2022-24785>

- CVE-2022-24903

<https://www.cve.org/CVERecord?id=CVE-2022-24903>

- CVE-2022-25647

<https://www.cve.org/CVERecord?id=CVE-2022-25647>

- CVE-2022-29622

<https://www.cve.org/CVERecord?id=CVE-2022-29622>

- CVE-2022-31129

<https://www.cve.org/CVERecord?id=CVE-2022-31129>

- CVE-2022-3715

<https://www.cve.org/CVERecord?id=CVE-2022-3715>

- CVE-2023-22067

<https://www.cve.org/CVERecord?id=CVE-2023-22067>

- CVE-2023-22081

<https://www.cve.org/CVERecord?id=CVE-2023-22081>

- CVE-2023-24998

<https://www.cve.org/CVERecord?id=CVE-2023-24998>

- CVE-2023-26159

<https://www.cve.org/CVERecord?id=CVE-2023-26159>

- CVE-2023-2976

<https://www.cve.org/CVERecord?id=CVE-2023-2976>

- CVE-2023-33850

<https://www.cve.org/CVERecord?id=CVE-2023-33850>

- CVE-2023-37466

<https://www.cve.org/CVERecord?id=CVE-2023-37466>

- CVE-2023-37903

<https://www.cve.org/CVERecord?id=CVE-2023-37903>

- CVE-2023-38552

<https://www.cve.org/CVERecord?id=CVE-2023-38552>

- CVE-2023-39331

<https://www.cve.org/CVERecord?id=CVE-2023-39331>

- CVE-2023-39332

<https://www.cve.org/CVERecord?id=CVE-2023-39332>

- CVE-2023-39333

<https://www.cve.org/CVERecord?id=CVE-2023-39333>

- CVE-2023-44483

<https://www.cve.org/CVERecord?id=CVE-2023-44483>

- CVE-2023-46749

<https://www.cve.org/CVERecord?id=CVE-2023-46749>

- CVE-2023-46750

<https://www.cve.org/CVERecord?id=CVE-2023-46750>

- CVE-2023-51775

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

- CVE-2023-52425

<https://www.cve.org/CVERecord?id=CVE-2023-52425>

- CVE-2023-52426

<https://www.cve.org/CVERecord?id=CVE-2023-52426>

- CVE-2023-5363

<https://www.cve.org/CVERecord?id=CVE-2023-5363>

- CVE-2023-5676

<https://www.cve.org/CVERecord?id=CVE-2023-5676>

- CVE-2024-1597

<https://www.cve.org/CVERecord?id=CVE-2024-1597>

- CVE-2024-20918

<https://www.cve.org/CVERecord?id=CVE-2024-20918>

- CVE-2024-20919

<https://www.cve.org/CVERecord?id=CVE-2024-20919>

- CVE-2024-20921

<https://www.cve.org/CVERecord?id=CVE-2024-20921>

- CVE-2024-20926

<https://www.cve.org/CVERecord?id=CVE-2024-20926>

- CVE-2024-20945

<https://www.cve.org/CVERecord?id=CVE-2024-20945>

- CVE-2024-20952

<https://www.cve.org/CVERecord?id=CVE-2024-20952>

- CVE-2024-21634

<https://www.cve.org/CVERecord?id=CVE-2024-21634>

- CVE-2024-25041

<https://www.cve.org/CVERecord?id=CVE-2024-25041>

- CVE-2024-25053

<https://www.cve.org/CVERecord?id=CVE-2024-25053>

- CVE-2024-27322

<https://www.cve.org/CVERecord?id=CVE-2024-27322>

- CVE-2024-28233

<https://www.cve.org/CVERecord?id=CVE-2024-28233>

- CVE-2024-28757

<https://www.cve.org/CVERecord?id=CVE-2024-28757>

- CVE CVE-2024-37532

<https://www.cve.org/CVERecord?id=CVE-2024-37532>