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

Autorité Nationale de Cybersécurité

Djibouti le, 09-06-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilité dans les produit IBM
Réference	1160
Date de Publication	2024-06-07
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
- Non spécifié par l'éditeur

SYSTÉME AFFECTÉ :

- AIX versions 7.2 et 7.3 sans la dernière version du fichier bind.rte
- Db2 versions 10.5.0 à 10.5.11 sans le dernier correctif de sécurité pour Tivoli System Automation for Multiplatforms (TSAMP)
- Db2 versions 11.1.4 à 11.1.4.7 sans le dernier correctif de sécurité pour TSAMP
- Db2 versions 11.5.0 à 11.1.5.9 sans le dernier correctif de sécurité pour TSAMP
- IBM Sterling Transformation Extender versions 10.1.0.x antérieures à 10.1.0.2 sans le correctif de sécurité PH61425
- IBM Sterling Transformation Extender versions 10.1.1.x antérieures à 10.1.1.1 sans le correctif de sécurité PH61425
- IBM Sterling Transformation Extender versions 10.1.2.x antérieures à 10.1.2.1 sans le correctif de sécurité PH61425
- IBM Sterling Transformation Extender versions 11.x antérieures à 11.0.0.0 sans le correctif de sécurité PH61425
- MaaS360 Mobile Enterprise Gateway (MEG) versions antérieures à 3.000.800
- MaaS360 VPN versions antérieures à 3.000.800
- QRadar SIEM versions 7.5.x antérieures à 7.5.0 UP8 IF03
- VIOS versions 3.1 et 4.1 sans la dernière version du fichier bind.rte

DÉSCRIPTION :

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

Ces vulnérabilités permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données.

SOLUTION :

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

DOCUMENTATION :

- Bulletin de sécurité IBM 7156255 du 03 juin 2024

https://www.ibm.com/support/pages/node/7156255

- Bulletin de sécurité IBM 7156292 du 03 juin 2024

https://www.ibm.com/support/pages/node/7156292

- Bulletin de sécurité IBM 7156443 du 04 juin 2024

https://www.ibm.com/support/pages/node/7156443

- Bulletin de sécurité IBM 7156525 du 05 juin 2024

https://www.ibm.com/support/pages/node/7156525

- Bulletin de sécurité IBM 7156667 du 06 juin 2024

https://www.ibm.com/support/pages/node/7156667

- CVE-2023-33850

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

- CVE-2023-3758

https://www.cve.org/CVERecord?id=CVE-2023-3758

- CVE-2023-38264

https://www.cve.org/CVERecord?id=CVE-2023-38264

- CVE-2023-40546

https://www.cve.org/CVERecord?id=CVE-2023-40546

- CVE-2023-40547

https://www.cve.org/CVERecord?id=CVE-2023-40547

- CVE-2023-40548

https://www.cve.org/CVERecord?id=CVE-2023-40548

- CVE-2023-40549

https://www.cve.org/CVERecord?id=CVE-2023-40549

- CVE-2023-40550

https://www.cve.org/CVERecord?id=CVE-2023-40550

- CVE-2023-40551

https://www.cve.org/CVERecord?id=CVE-2023-40551

- CVE-2023-4408

https://www.cve.org/CVERecord?id=CVE-2023-4408

- CVE-2023-50387

https://www.cve.org/CVERecord?id=CVE-2023-50387

- CVE-2023-50868

https://www.cve.org/CVERecord?id=CVE-2023-50868

- CVE-2023-5517

https://www.cve.org/CVERecord?id=CVE-2023-5517

- CVE-2023-5679

https://www.cve.org/CVERecord?id=CVE-2023-5679

- CVE-2023-6129

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

- CVE-2023-6237

https://www.cve.org/CVERecord?id=CVE-2023-6237

- CVE-2023-6516

https://www.cve.org/CVERecord?id=CVE-2023-6516

- CVE-2024-0727

https://www.cve.org/CVERecord?id=CVE-2024-0727

- 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-2024-21011

https://www.cve.org/CVERecord?id=CVE-2024-21011

- CVE-2024-21085

https://www.cve.org/CVERecord?id=CVE-2024-21085

- CVE-2024-21094

https://www.cve.org/CVERecord?id=CVE-2024-21094

- CVE-2024-22201

https://www.cve.org/CVERecord?id=CVE-2024-22201

- CVE-2024-22243

https://www.cve.org/CVERecord?id=CVE-2024-22243

- CVE-2024-22259

https://www.cve.org/CVERecord?id=CVE-2024-22259

- CVE-2024-22262

https://www.cve.org/CVERecord?id=CVE-2024-22262

- CVE-2024-29025

https://www.cve.org/CVERecord?id=CVE-2024-29025