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

Autorité Nationale de Cybersécurité

Djibouti le, 24-02-2026

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits IBM
Réference	1421
Date de Publication	2026-02-24
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 7.2.5 sans le correctif de sécurité IJ57162
- AIX versions 7.3.2 sans le correctif de sécurité IJ57231
- AIX versions 7.3.3 sans le correctif de sécurité IJ57128
- AIX versions 7.3.4 sans le correctif de sécurité IJ57232
- Sterling External Authentication Server versions 6.1.0.x antérieures à 6.1.0.4 GA
- Sterling External Authentication Server versions 6.1.1.x antérieures à 6.1.1.2 GA
- Sterling Secure Proxy versions 6.1.x antérieures à 6.1.0.3 GA
- Sterling Secure Proxy versions 6.2.0.x antérieures à 6.2.0.3 GA
- Sterling Secure Proxy versions 6.2.1.x antérieures à 6.2.1.1 GA
- Sterling Transformation Extender versions 10.1.0.2 sans le correctif APAR PH69842
- Sterling Transformation Extender versions 10.1.1.1 sans le correctif APAR PH69842
- Sterling Transformation Extender versions 10.1.2.1 sans le correctif APAR PH69842
- Sterling Transformation Extender versions 11.0.0.0 sans le correctif APAR PH69842
- VIOS versions 4.1.0 sans le correctif de sécurité IJ57231
- VIOS versions 4.1.1 sans le correctif de sécurité IJ57128
- VIOS versions 4.1.2 sans le correctif de sécurité IJ57232

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans les produits IBM. Certaines peuvent être exploitées par un attaquant pour exécuter du code arbitraire à distance, provoquer un déni de service à distance ou compromettre la confidentialité des données.

SOLUTION :

Consulter le bulletin de sécurité de l’éditeur afin d’obtenir les correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité IBM 7261039 du 17 février 2026

https://www.ibm.com/support/pages/node/7261039

- Bulletin de sécurité IBM 7261040 du 17 février 2026

https://www.ibm.com/support/pages/node/7261040

- Bulletin de sécurité IBM 7261053 du 17 février 2026

https://www.ibm.com/support/pages/node/7261053

- Bulletin de sécurité IBM 7261181 du 18 février 2026

https://www.ibm.com/support/pages/node/7261181

- Bulletin de sécurité IBM du 19 février 2026

https://www.ibm.com/support/pages/node/7261396

- Référence CVE CVE-2025-12816

https://www.cve.org/CVERecord?id=CVE-2025-12816

- Référence CVE CVE-2025-15284

https://www.cve.org/CVERecord?id=CVE-2025-15284

- Référence CVE CVE-2025-48734

https://www.cve.org/CVERecord?id=CVE-2025-48734

- Référence CVE CVE-2025-48924

https://www.cve.org/CVERecord?id=CVE-2025-48924

- Référence CVE CVE-2025-53057

https://www.cve.org/CVERecord?id=CVE-2025-53057

- Référence CVE CVE-2025-53066

https://www.cve.org/CVERecord?id=CVE-2025-53066

- Référence CVE CVE-2025-58754

https://www.cve.org/CVERecord?id=CVE-2025-58754

- Référence CVE CVE-2025-62230

https://www.cve.org/CVERecord?id=CVE-2025-62230

- Référence CVE CVE-2025-62231

https://www.cve.org/CVERecord?id=CVE-2025-62231

- Référence CVE CVE-2025-64756

https://www.cve.org/CVERecord?id=CVE-2025-64756

- Référence CVE CVE-2025-66030

https://www.cve.org/CVERecord?id=CVE-2025-66030

- Référence CVE CVE-2025-66031

https://www.cve.org/CVERecord?id=CVE-2025-66031

- Référence CVE CVE-2025-8885

https://www.cve.org/CVERecord?id=CVE-2025-8885

- Référence CVE CVE-2025-8916

https://www.cve.org/CVERecord?id=CVE-2025-8916

- Référence CVE CVE-2026-21925

https://www.cve.org/CVERecord?id=CVE-2026-21925

- Référence CVE CVE-2026-21932

https://www.cve.org/CVERecord?id=CVE-2026-21932

- Référence CVE CVE-2026-21933

https://www.cve.org/CVERecord?id=CVE-2026-21933

- Référence CVE CVE-2026-21945

https://www.cve.org/CVERecord?id=CVE-2026-21945