AVIS DE SECURITE

Objet	**Multiples vulnérabilités dans les produits IBM (MQ, Verify Identity Access / Security Verify Access, TRIRIGA Application Platform)**
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-274
TLP	WHITE

Résumé

IBM a publié les 19 et 20/10/2026 des bulletins de sécurité corrigeant plusieurs vulnérabilités de score CVSS v3.1 de 8.8 : un dépassement de tampon dans le traitement MQPUT d'IBM MQ (CVE-2026-10572), des identifiants codés en dur dans IBM Verify Identity Access / Security Verify Access (CVE-2026-109126) et une authentification défaillante dans IBM TRIRIGA Application Platform (CVE-2026-107400).

Ces failles peuvent conduire à une exécution de code arbitraire, à un déni de service ou à une élévation de privilèges. Aucune exploitation active n'est signalée à ce jour.

Risque de sécurité

- Exécution de code arbitraire à distance (utilisateur authentifié)
- Déni de service
- Élévation de privilèges (identifiants codés en dur)
- Contournement de la politique de sécurité (authentification)

Systèmes affectés

- IBM MQ Operator : 2.0.0 à 2.0.29, 3.2.0 à 3.2.29, 3.3.0 à 3.4.0 (exclu), 3.4.1, 3.5.0 à 3.5.3, 3.6.0 à 3.6.4, 3.7.0 à 3.7.2, 3.8.0 à 3.8.1, 3.9.0 à 3.9.2, 4.0.0 à 4.0.4
- Images conteneur IBM MQ Advanced (9.3.x LTS, 9.4.x CD, 10.0.0.x) : se référer à la liste détaillée du bulletin IBM
- IBM Verify Identity Access 11.0.3.1
- IBM Security Verify Access 10.0.9.3 (appliance)
- IBM TRIRIGA Application Platform 5.0.0 à 5.0.8

Recommandations

Se référer aux bulletins de sécurité de l'éditeur du 20/10/2026 et appliquer les correctifs ou mises à jour indiqués :

- https://www.ibm.com/support/pages/node/7292667
- https://www.ibm.com/support/pages/node/7292606
- https://www.ibm.com/support/pages/node/7292418
- https://nvd.nist.gov/vuln/detail/CVE-2026-10572
- https://nvd.nist.gov/vuln/detail/CVE-2026-109126
- https://nvd.nist.gov/vuln/detail/CVE-2026-107400