AVIS DE SECURITE

Objet	Vulnérabilité critique de révocation de session dans l'API Core d'Apache Airflow
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-220
TLP	WHITE

Résumé

Apache a publié le 21 septembre 2026 la version 3.3.2 d'Apache Airflow corrigeant la vulnérabilité CVE-2026-86473 (CVSS v3.1 9.1). Le point de terminaison de déconnexion de l'API Core ne révoque que le jeton de session présenté dans le cookie _token : lorsqu'un client se déconnecte en présentant son jeton via l'en-tête Authorization Bearer, aucune révocation n'est effectuée et le jeton reste valide jusqu'à son expiration (24 heures par défaut). Un attaquant détenant une copie du jeton conserve ainsi l'accès de la victime après sa déconnexion. La même version corrige deux vulnérabilités de sévérité moyenne (CVE-2026-75158 et CVE-2026-82355). Ce bulletin est distinct du bulletin SNCSIRT-2026-ADS-216 portant sur le fournisseur FAB.

Risque de sécurité

- Contournement de la politique de sécurité : maintien d'une session après déconnexion (CVE-2026-86473, CVSS 9.1)
- Atteinte à la confidentialité et à l'intégrité des workflows orchestrés
- Atteinte à la confidentialité des données : énumération d'événements d'assets de DAG non autorisés (CVE-2026-75158, CVSS 4.3)
- Usurpation d'identité / confusion de principal par fixation de session (CVE-2026-82355, CVSS 4.2, versions 3.3.0 et 3.3.1)

Systèmes affectés

- Apache Airflow versions 3.0.0 à 3.3.1 (paquet apache-airflow)
- Clients de l'API Core s'authentifiant par jeton Bearer plutôt que par cookie de session

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 21 septembre 2026 :

   - https://lists.apache.org/thread/k9z1p0q1ng8m68nlnv9d1fqzscrfm7vr (avis Apache Airflow — CVE-2026-86473)
   - https://lists.apache.org/thread/rx5lg86l0qkjl2s7dtmpqxjq0xplr4fy (CVE-2026-75158) ; https://lists.apache.org/thread/3p7zpdvv40tn01m0xk5mt2rxg88mw8w1 (CVE-2026-82355)
   - https://nvd.nist.gov/vuln/detail/CVE-2026-86473 (référence NVD)

2. Mettre à niveau Apache Airflow vers la version 3.3.2 ou ultérieure ; en attendant, réduire la durée de vie des jetons et révoquer les jetons potentiellement exposés