AVIS DE SECURITE

Objet	Multiples vulnérabilités critiques dans le fournisseur FAB (Flask-AppBuilder) d'Apache Airflow
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-216
TLP	WHITE

Résumé

Apache a publié le 16 septembre 2026 quatre avis de sécurité concernant le fournisseur FAB (Flask-AppBuilder) d'Apache Airflow (paquet apache-airflow-providers-fab), utilisé pour l'authentification et la gestion des sessions de la plateforme d'orchestration de workflows Apache Airflow. Les deux vulnérabilités les plus critiques, CVE-2026-82311 (CVSS 9.8) et CVE-2026-86462 (CVSS 9.1), permettent à un attaquant en possession d'un cookie de session compromis de conserver un accès complet au compte de la victime même après une réinitialisation ou une modification de son mot de passe par un administrateur, en raison d'un défaut d'invalidation des sessions actives en base de données. Deux vulnérabilités additionnelles affectent le même composant : CVE-2026-86466 (CVSS 8.1), un défaut de validation du jeton OAuth du fournisseur d'identité Authentik permettant une usurpation d'utilisateur, et CVE-2026-82310 (CVSS 7.2), qui permet à un compte désactivé par un administrateur de conserver un accès via un jeton API existant. Aucune exploitation active n'est signalée à ce jour pour ces quatre CVE.

Risque de sécurité

- Contournement de la politique de sécurité : maintien d'accès à un compte après réinitialisation du mot de passe par un administrateur (CVE-2026-82311, CVSS 9.8)
- Contournement de la politique de sécurité : maintien d'accès à un compte après modification du mot de passe via l'API d'administration (CVE-2026-86462, CVSS 9.1)
- Usurpation d'identité / contournement d'authentification via un jeton OAuth (fournisseur Authentik) dont l'audience n'est pas validée (CVE-2026-86466, CVSS 8.1)
- Élévation de privilèges : maintien d'accès d'un compte pourtant désactivé par un administrateur, via un jeton API existant non révoqué (CVE-2026-82310, CVSS 7.2)
- Accès non autorisé à l'interface d'administration d'Apache Airflow et atteinte à la confidentialité et à l'intégrité des workflows orchestrés

Systèmes affectés

- apache-airflow-providers-fab versions ≥ 2.4.2 et < 3.9.0 (CVE-2026-82311, CVE-2026-82310)
- apache-airflow-providers-fab versions ≥ 3.2.0 et < 3.9.0 (CVE-2026-86462)
- apache-airflow-providers-fab versions < 3.9.0 utilisant le fournisseur d'authentification OAuth Authentik (CVE-2026-86466)
- Déploiements Apache Airflow utilisant le gestionnaire d'authentification FAB (FAB auth manager) avec sessions persistées en base de données ([fab] session_backend=database) pour CVE-2026-82311 et CVE-2026-86462

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 16 septembre 2026 :
   - https://lists.apache.org/thread/mmplwl93shy615shkpp9p4fzyjvr4yqw (avis Apache Airflow — CVE-2026-82311)
   - https://lists.apache.org/thread/7sr4sggfv5fhhl3qgphcq0rlhg81do1s (avis Apache Airflow — CVE-2026-86462)
   - https://lists.apache.org/thread/qh7fobs16p2hgln2yblbgf8ty4dvf4y7 (avis Apache Airflow — CVE-2026-86466)
   - https://github.com/advisories/ghsa-6fx3-rxq6-j8w2 (avis GitHub Security Advisory — CVE-2026-86466)
   - https://nvd.nist.gov/vuln/detail/CVE-2026-82311 ;
   - https://nvd.nist.gov/vuln/detail/CVE-2026-86462 (références NVD)
2. Mettre à niveau le paquet apache-airflow-providers-fab vers la version 3.9.0 ou ultérieure, qui corrige l'ensemble des quatre vulnérabilités