AVIS DE SECURITE

Objet	Vulnérabilité critique d'exécution de code à distance dans F5 BIG-IP Access Policy Manager (APM)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-217
TLP	WHITE

Résumé

F5 a publié le 22 septembre 2026 des correctifs pour la vulnérabilité CVE-2026-94127 (CVSS v3.1 9.8), un débordement de tampon dans le tas (CWE-122) affectant F5 BIG-IP Access Policy Manager (APM). La faille est déclenchable à distance, sans authentification ni interaction utilisateur, sur un serveur virtuel configuré simultanément avec une politique d'accès APM et un profil OAuth, et permet l'exécution de code arbitraire sur le plan de données (TMM). La vulnérabilité est activement exploitée et a été ajoutée au catalogue CISA KEV le 22 septembre 2026.

Risque de sécurité

- Exécution de code arbitraire à distance sans authentification (CVE-2026-94127, CVSS 9.8)
- Atteinte à la confidentialité et à l'intégrité des flux d'authentification traités par la passerelle
- Déni de service à distance (plantage du microkernel TMM)
- Compromission de la passerelle d'accès et rebond vers le système d'information interne

Systèmes affectés

- BIG-IP APM 21.1.0 (corrigé par Hotfix-BIGIP-21.1.0.2.0.30.22)
- BIG-IP APM 17.5.0 à 17.5.1 (corrigé par Hotfix-BIGIP-17.5.1.9.0.160.12)
- BIG-IP APM 17.1.0 à 17.1.3 (corrigé par Hotfix-BIGIP-17.1.3.5.0.41.14)
- Seuls les serveurs virtuels configurés avec à la fois une politique d'accès APM et un profil OAuth sont exposés (y compris en mode Appliance)

Recommandations

1. Se référer au bulletin de sécurité de l'éditeur du 22 septembre 2026 :
   - https://my.f5.com/manage/s/article/K000162605 (avis F5 K000162605 — CVE-2026-94127)
   - https://www.cisa.gov/news-events/alerts/2026/09/22/cisa-adds-four-known-exploited-vulnerabilities-catalog
2. Appliquer en priorité le hotfix d'ingénierie correspondant à la branche utilisée ; à défaut, déployer l'iRule de mitigation fournie par le support F5
3. Rechercher les indicateurs publiés par F5 (échecs répétés d'authentification OAuth, commandes suspectes, plantages du TMM) et engager une investigation en cas de compromission suspectée