AVIS DE SECURITE

Objet	Multiples vulnérabilités critiques dans HPE Aruba Networking EdgeConnect SD-WAN (Gateways et Orchestrator)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-208
TLP	WHITE

Résumé

HPE a publié le 15 septembre 2026 le bulletin de sécurité HPESBNW05135 corrigeant de multiples vulnérabilités critiques dans les gateways et l'orchestrateur EdgeConnect SD-WAN. Les failles les plus sévères (CVE-2026-76669 et CVE-2026-76670, CVSS 9.9) sont des contournements d'autorisation dans l'API de l'Orchestrator SD-WAN EdgeConnect, permettant à un attaquant authentifié à faible privilège d'élever ses droits jusqu'au niveau administrateur. Une vulnérabilité de débordement de tampon non authentifiée (CVE-2026-76674, CVSS 9.8) permet en outre l'exécution de code arbitraire à distance sur les gateways. HPE recommande l'installation immédiate des correctifs disponibles.

Risque de sécurité

- Élévation de privilèges jusqu'au niveau administrateur (CVE-2026-76669, CVE-2026-76670, CVSS 9.9)
- Divulgation d'informations sensibles via un point de terminaison de synchronisation de cache (CVE-2026-76672, CVSS 9.9)
- Exécution de code arbitraire à distance non authentifiée par débordement de tampon (CVE-2026-76674, CVSS 9.8)
- Atteinte à la confidentialité et à l'intégrité des données
- Déni de service à distance
- Falsification de requêtes côté serveur (SSRF)

Systèmes affectés

- EdgeConnect SD-WAN Gateways versions 9.4.x.x antérieures à ECOS 9.4.9.0
- EdgeConnect SD-WAN Gateways versions 9.5.x.x antérieures à ECOS 9.5.9.0
- EdgeConnect SD-WAN Gateways versions 9.6.x.x antérieures à ECOS 9.6.4.0
- EdgeConnect SD-WAN Gateways versions 9.7.x.x antérieures à ECOS 9.7.1.0
- EdgeConnect SD-WAN Orchestrator versions 9.4.x antérieures à Orchestrator 9.4.11
- EdgeConnect SD-WAN Orchestrator versions 9.5.x antérieures à Orchestrator 9.5.9
- EdgeConnect SD-WAN Orchestrator versions 9.6.x antérieures à Orchestrator 9.6.4
- EdgeConnect SD-WAN Orchestrator versions 9.7.x antérieures à Orchestrator 9.7.1

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 15 septembre 2026 :

- https://csaf.arubanetworking.hpe.com/2026/hpe_networking_-_hpesbnw05135.txt