AVIS DE SECURITE

Objet	Vulnérabilité critique zero-day dans Check Point Security Management et exploitation active de CVE-2026-85102 (CISA KEV)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-218
TLP	WHITE

Résumé

Check Point a publié le 22 septembre 2026 un avis de sécurité signalant l'exploitation active de deux vulnérabilités critiques. CVE-2026-93616 (CVSS 9.8) est une vulnérabilité zero-day de traversée de répertoire non authentifiée dans le service web de Check Point Security Management, permettant d'exécuter un script depuis un chemin arbitraire et de charger une classe Java arbitraire ; des attaques ciblées ont été observées. Par ailleurs, CVE-2026-85102 (CVSS 9.8, exécution de code à distance via la validation des certificats VPN des Security Gateway), corrigée le 9 septembre 2026 et déjà traitée par le bulletin SNCSIRT-2026-ADS-195, fait désormais l'objet d'une vague d'exploitation. Les deux CVE ont été ajoutées au catalogue CISA KEV le 22 septembre 2026.

Risque de sécurité

- Exécution de code arbitraire à distance sans authentification sur le serveur de management (CVE-2026-93616, CVSS 9.8)
- Exécution de code arbitraire à distance sans authentification sur les passerelles VPN (CVE-2026-85102, CVSS 9.8)
- Compromission de la politique de sécurité de l'ensemble des pare-feux gérés
- Atteinte à la confidentialité et à l'intégrité des données

Systèmes affectés

- Security Management (CVE-2026-93616) : R82.20 ; R82.10 Jumbo Hotfix Take 44 ou inférieur ; R82 Jumbo Hotfix Take 126 ou inférieur ; R81.20 Jumbo Hotfix Take 166 ou inférieur ; R81.10 Jumbo Hotfix Take 190 ou inférieur (fin de support) ; R80 à R81 (fin de support)
- Produits concernés par CVE-2026-93616 : Security Management Server, Multi-Domain Security Management Server, Log Server, Multi-Domain Log Server, SmartEvent
- Security Gateway et Spark Firewall (CVE-2026-85102) : R81, R81.10, R81.10.X, R81.20, R82, R82.00.X, R82.10 sans le correctif du 9 septembre 2026
- Note : Check Point LivePatch Take 28/29 ne corrige pas CVE-2026-93616

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 22 septembre 2026 :
   - https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616 (avis Check Point)
   - https://support.checkpoint.com/results/sk/sk1000171 (CVE-2026-93616 — correctifs, mitigation, indicateurs de compromission)
   - https://support.checkpoint.com/results/sk/sk1000117 (CVE-2026-85102)
   - https://www.cisa.gov/news-events/alerts/2026/09/22/cisa-adds-four-known-exploited-vulnerabilities-catalog (ajout au catalogue CISA KEV)

2. En mitigation temporaire, restreindre l'accès au serveur de management aux seules adresses IP de confiance (SmartConsole > Manage & Settings > Permissions & Administrators > Trusted Clients) et rechercher les connexions Mobile Access anormales par certificat