Quentin Duret

Veille technologique – Cybersécurité

Une vulnérabilité critique (CVE-2026-59310) touchant VMware vCenter Server est actuellement exploitée par des groupes de ransomware. Elle permet l'exécution de commandes à distance (RCE) et la prise de contrôle potentielle de l'ensemble de l'infrastructure virtuelle. Bien qu'un patch ait été publié le 29 juillet 2026, de nombreux serveurs non mis à jour ont été compromis dès le mois d'août (plus de 360 serveurs touchés dans 47 pays).

Action immédiate:

Appliquer le patch : Mettre à jour VMware vCenter immédiatement avec la version corrigée fournie par l'éditeur. Audit & Recherche d'intrusion : Inspecter les serveurs exposés pour détecter toute présence d'accès non autorisé ou de backdoor résiduelle.

Bonnes pratiques de sécurisation:

Isolation : Retirer l'accès direct à vCenter depuis Internet (rendre vCenter accessible uniquement via VPN / Réseau interne). Segmentation : Séparer le réseau d'administration du reste du réseau de l'entreprise. Moindre privilège : Restreindre les comptes disposant des droits d'administration. Supervision : Surveiller activement les connexions et comportements inhabituels sur vCenter. Sauvegardes : Maintenir des sauvegardes hors-ligne (air-gapped) et isolées du réseau principal.

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017?utm_ https://www.shadowserver.org/what-we-do/network-reporting/vmware-vcenter-cve-2026-59310-exploitation-victim-special-report/?utm_ https://labs.cloudsecurityalliance.org/research/csa-research-note-vmware-vcenter-cve-2026-59310-exploitation/?utm_ https://www.bleepingcomputer.com/news/security/cisa-critical-vmware-vcenter-rce-flaw-now-exploited-by-ransomware-gangs/?utm_