VEILLE TECHNOLOGIQUE • SÉCURISATION D'ACTIVE DIRECTORY — FICHE 4

Kerberos : la faille CheckSum et la fin définitive de RC4

Date de la veille : 10 juin 2026

Pour cette dernière veille axée sur Kerberos, j'ai croisé deux évolutions majeures : la correction de la faille *CheckSum* (**CVE-2025-60704**, score CVSS 7,5) et le retrait progressif du chiffrement RC4 (**CVE-2026-20833**). Alors que *CheckSum* permettait à un attaquant en position d'homme du milieu d'usurper une identité via la délégation Kerberos, Microsoft a parallèlement enclenché la fin définitive de RC4 entre janvier et juillet 2026 au profit de l'**AES**.

Ce qu'il faut retenir, c'est que RC4 était la principale faiblesse exploitée lors des attaques par *Kerberoasting*, permettant de casser hors ligne les mots de passe des comptes de service. Son retrait renforce donc nettement l'authentification du domaine, mais déplace le risque vers la disponibilité : les anciens équipements ou NAS incapables de gérer l'AES risquent de perdre l'accès au domaine.

Côté administration, appliquer les patchs ne suffit pas : il faut surveiller les événements système (201 à 207) et réinitialiser les mots de passe des vieux comptes de service pour forcer la génération de clés AES.

SOURCES

- Microsoft — *What is going on with RC4 in Kerberos?* (mis à jour le 10 juin 2026)
- Silverfort — *You Win Some, You CheckSum (CVE-2025-60704)*
- Rain City Tech — *Kerberos RC4 enforcement (CVE-2026-20833)*