Rapport d’Audit Sécurité

Vulnérabilité Linux Kernel 0-Day « Copy Fail »

Destinataire : RSSI / Équipe Sécurité

Classification : Critique

Résumé exécutif

La vulnérabilité Copy Fail permet une élévation de privilèges root sur de nombreux systèmes Linux. Elle est simple à exploiter, invisible aux outils classiques et nécessite une correction immédiate.

Description technique

Bug logique dans l'interface AF_ALG combinée à splice(). Manipulation du page cache permettant modification mémoire sans trace disque.

Impact

Accès root local, compromission de serveurs, escape de conteneurs et propagation dans des environnements cloud.

Détection

Analyse du kernel, présence AF_ALG, modules chargés et tests comportementaux.

Remédiation

Mise à jour kernel, désactivation AF_ALG, hardening système et activation LSM.

Recommandations

Mettre à jour immédiatement, auditer tous les systèmes, renforcer la sécurité et surveiller les accès.

Évaluation du risque

Critère	Niveau
Exploitabilité	Très élevée
Complexité	Faible
Impact	Critique
Détection	Faible
Portabilité	Élevée