AVIS DE SECURITE

Objet	**Multiples vulnérabilités dans le noyau Linux de Red Hat (Red Hat Enterprise Linux)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-269
TLP	WHITE

Résumé

Red Hat a publié entre le 09/10/2026 et le 14/10/2026 plusieurs bulletins de sécurité (RHSA) corrigeant 58 vulnérabilités dans le noyau Linux de Red Hat Enterprise Linux. Parmi elles, CVE-2026-64385 (double libération de mémoire dans le client SMB du noyau, CVSS v3.1 9.8) peut permettre à un attaquant distant d'exécuter du code arbitraire, et d'autres failles (ex. CVE-2026-68108, CVSS 8.8 ; CVE-2026-80521, CVSS 7.8) permettent une élévation de privilèges locale.

Risque de sécurité

- Exécution de code arbitraire à distance
- Élévation de privilèges
- Déni de service à distance
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données
- Contournement de la politique de sécurité

Systèmes affectés

- Red Hat Enterprise Linux 7 (ELS), 8, 8.10 (ELS), 9, 9.2, 9.4, 9.8, 10 et 10.2, y compris leurs variantes EUS, AUS, 4 years of updates et Update Services for SAP Solutions (x86_64, aarch64, s390x, ppc64le)
- Red Hat CodeReady Linux Builder 8, 9, 10 (dont EUS 9.8 et 10.2)
- Red Hat Enterprise Linux for Real Time 8 et 7 (ELS), dont la variante NFV pour la version 8

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 09/10/2026 au 14/10/2026 :
   - https://access.redhat.com/errata/RHSA-2026:79786 (09/10/2026)
   - https://access.redhat.com/errata/RHSA-2026:81349, RHSA-2026:81371, RHSA-2026:81406, RHSA-2026:81552 (12/10/2026)
   - https://access.redhat.com/errata/RHSA-2026:82806, RHSA-2026:82807, RHSA-2026:82860, RHSA-2026:83156, RHSA-2026:83157, RHSA-2026:83159, RHSA-2026:83207 (14/10/2026)