AVIS DE SECURITE

Objet	**Vulnérabilité critique d'exécution de code à distance dans le noyau Linux (pile TCP IPv4)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-300
TLP	WHITE

Résumé

Une vulnérabilité de type use-after-free (CVE-2026-98432, CVSS v3.1 : 9.8) affecte le sous-système réseau IPv4 du noyau Linux depuis la version 4.4. Une condition de concurrence lors du traitement des demandes de connexion TCP retransmises ou de la migration de sockets entraîne la libération prématurée des options IP encore en cours d'utilisation. Un attaquant distant non authentifié peut l'exploiter, sans interaction de l'utilisateur, pour provoquer un déni de service, une corruption de la mémoire du noyau ou une exécution de code à distance ; tout système acceptant des connexions TCP IPv4 entrantes est exposé, que MPTCP soit activé ou non. Red Hat a publié des noyaux corrigés le 01/11/2026, tandis que les correctifs Ubuntu sont en cours de publication.

Risque de sécurité

- Exécution de code arbitraire à distance (privilèges noyau)
- Déni de service à distance (plantage du système)
- Atteinte à la confidentialité des données (lecture de la mémoire du noyau)
- Atteinte à l'intégrité du système (corruption de la mémoire du noyau)

Systèmes affectés

- Noyau Linux à partir de la version 4.4, versions antérieures à 5.10.272, 5.15.223, 6.1.190, 6.6.159, 6.12.113, 6.18.56, 7.2.10 et 7.3 selon la branche
- Red Hat Enterprise Linux 8, 9 et 10, Red Hat OpenShift Container Platform 4 (nœuds RHEL CoreOS) et produits reposant sur le noyau RHEL
- Versions corrigées RHEL : kernel-4.18.0-553.182.1.el8_10 (RHSA-2026:93414), kernel-5.14.0-687.64.1.el9_8 (RHSA-2026:93412), kernel-6.12.0-211.72.1.el10_2 (RHSA-2026:93413)
- Ubuntu 16.04 LTS à 26.10 (paquet linux et noyaux dérivés) : vulnérables, correctifs en cours de publication ; Ubuntu 14.04 LTS non affecté
- Autres distributions (Debian, SUSE, Oracle Linux, Amazon Linux, AlmaLinux, Rocky Linux) : se référer aux avis de chaque éditeur

Recommandations

1. Mettre à jour le noyau vers une version corrigée puis redémarrer, en priorité les systèmes exposés acceptant des connexions TCP entrantes ;
2. Dans l'attente du correctif (notamment sous Ubuntu), appliquer la mesure d'atténuation nftables de Red Hat rejetant les paquets TCP IPv4 porteurs d'options IP : elle réduit l'exposition sans la supprimer et doit être réappliquée après chaque redémarrage.
3. Se référer aux bulletins de sécurité des éditeurs (Red Hat RHSB-2026-016 du 30/10/2026, mis à jour le 04/11/2026) :

- https://access.redhat.com/security/vulnerabilities/RHSB-2026-016
- https://access.redhat.com/security/cve/cve-2026-98432
- https://ubuntu.com/security/CVE-2026-98432
- https://nvd.nist.gov/vuln/detail/cve-2026-98432