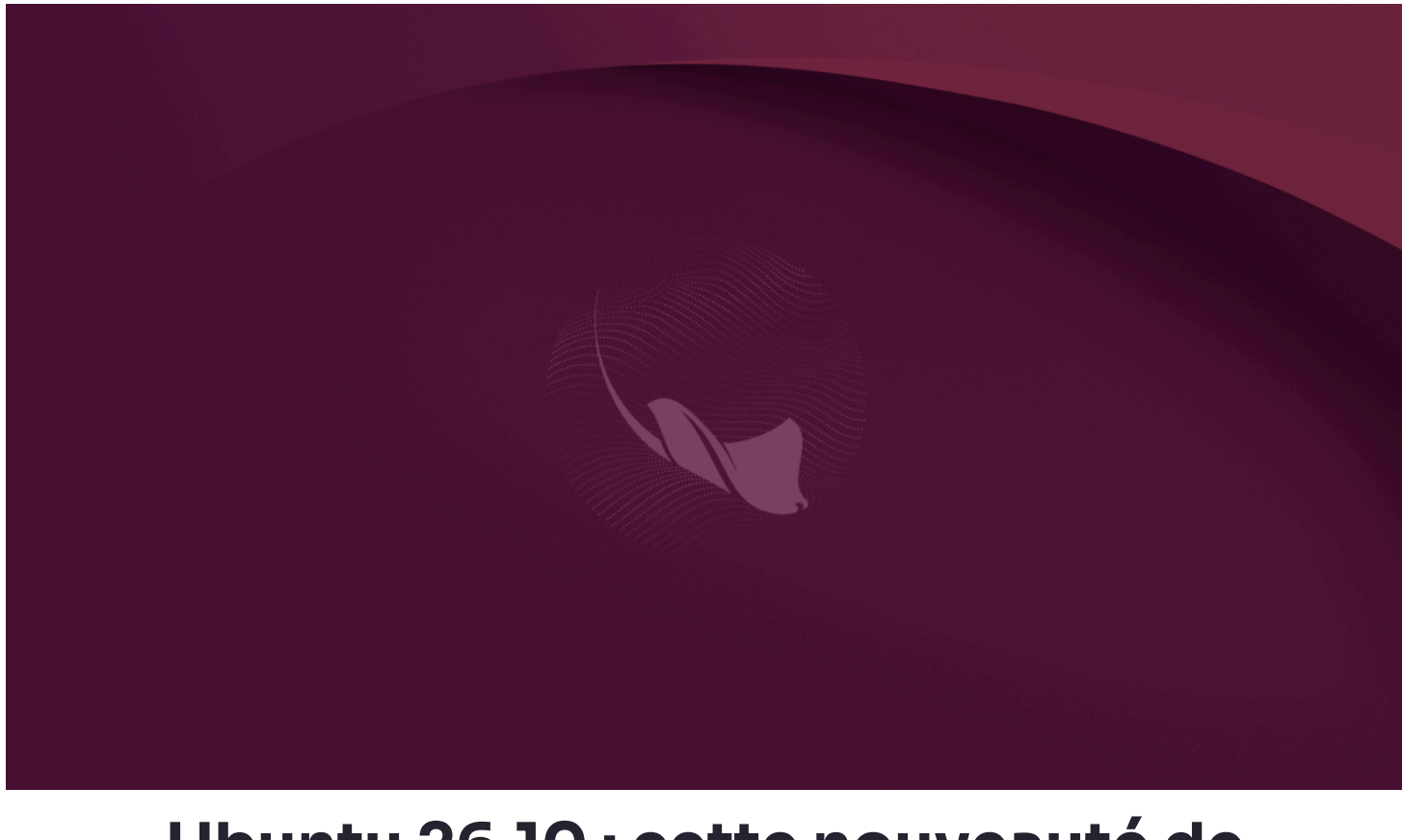




Ubuntu 26.10 : cette nouveauté de démarrage risque de bloquer votre PC

09/10/2026 / Applications À la une / 3 minutes de lecture

Canonical s’apprête à sacrifier la compatibilité historique de son système d’exploitation sur l’autel de la cybersécurité. À l’approche de la sortie officielle d’Ubuntu 26.10 (« Stonking Stingray ») ce 15 octobre, l’éditeur britannique tranche dans le vif : pour empêcher les outils d’IA offensive d’exploiter les failles de bas niveau, le chargeur de démarrage GRUB subit une amputation drastique sous Secure Boot. Revers de la médaille : des milliers de machines dotées de configurations de stockage avancées risquent de se retrouver purement et simplement bloquées lors de la mise à niveau.

La nouvelle est tombée ce 6 octobre dans un bullet de sécurité officiel sur le blog de Canonical . Ubuntu 26.10 “Stonking Stingray” présente un chargeur de démarrage allégé.

💡 En résumé

- **Élagage massif de GRUB** : Canonical supprime les pilotes Btrfs, ZFS, XFS ainsi que le support de LUKS et LVM de son binaire signé pour réduire la surface d’attaque sous Secure Boot.
- **Risque de blocage système** : les postes utilisant une partition /boot personnalisée sur ces formats seront empêchés de migrer vers 26.10 sans repartitionnement préalable.
- **Virage tout-Rust et quantique** : la distribution finalise la bascule de ses utilitaires système (cp, mv, rm) en Rust et déploie OpenSSL 4.0 avec chiffrement post-quantique.

La traque aux failles Secure Boot impose une purge logicielle

Le constat dressé par Canonical dans ses notes techniques est sans appel : les générateurs de vulnérabilités accélérés par l’IA multiplient les attaques contre les analyseurs de code exécutés avant le chargement du noyau. Historiquement, le chargeur **GRUB** embarquait une multitude de modules pour décoder des systèmes de fichiers exotiques ou afficher des images de démarrage. Chacun de ces interpréteurs constituait une brèche potentielle pour contourner la signature cryptographique du matériel.

Pour fermer ces portes dérobées, la version signée distribuée avec Ubuntu 26.10 ne conserve que le strict minimum opérationnel :

- **Systèmes de fichiers maintenus** : seules les partitions de démarrage au format **ext4**, **FAT**, **ISO9660** et les conteneurs **squashfs** pour les paquets Snap restent autorisés sous Secure Boot.
- **Pilotes évincés du binaire signé** : suppression totale des modules Btrfs, ZFS, XFS, HFS+, du décodage des images JPEG et PNG, ainsi que des tables de partitionnement Apple.
- **Architectures de stockage exclues** : l’exécution de /boot sur des volumes logiques **LVM**, du RAID logiciel (hors RAID1) et le chiffrement **LUKS** sont désormais rejetés par le chemin d’amorçage signé.
- **Comportement après le démarrage** : ces technologies continuent de fonctionner parfaitement une fois le noyau Linux 7.3 chargé, ou lorsque Secure Boot est volontairement désactivé dans le microprogramme UEFI.

L’arsenal défensif

Ce durcissement du chargeur s’accompagne d’une refonte en profondeur des briques de base de l’OS. Après avoir amorcé la transition sur la version 26.04 LTS, Ubuntu 26.10 achève la migration de ses commandes fondamentales vers le langage **Rust** : les utilitaires historiques cp, mv et rm abandonnent définitivement le code C de GNU Coreutils pour neutraliser les erreurs de corruption de mémoire vive.

L’infrastructure réseau et cryptographique fait un saut générationnel avec l’intégration d’**OpenSSL 4.0** et d’**OpenSSH 10.5**, activant par défaut des mécanismes d’échange de clés hybrides résistants aux futurs calculateurs quantiques. Le vieux démon dbus-daemon, en fonction depuis 2004, cède quant à lui sa place à **dbus-broker** pour fiabiliser le bus de communication système sous le contrôle strict des profils **AppArmor**.

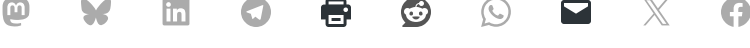
Les utilisateurs disposant d’installations complexes sur leurs postes devront vérifier leur agencement de disques avant le déploiement général prévu le 15 octobre, sous peine de devoir rester sur le cycle long Ubuntu 26.04 LTS pour éviter tout refus d’amorçage.

🌐 **L’actualité de l’open source et des technologies éthiques dans votre flux**

🐼 **Fediverse / Mastodon** : suivez notre profil officiel @redaction@goodtech.info depuis votre application ou votre instance favorite.

🦋 **Bluesky (AT Protocol)** : retrouvez nos actualités condensées et abonnez-vous à @goodtech.info .

Allez-y, partagez !



J’aime ça :

J’aime Soyez le premier à aimer cet article.

Articles similaires

- Vie privée garantie : Canonical dévoile Myna, l’outil de dictée IA 100% local d’Ubuntu 🐸

19 juin 2026

Dans "Applications"
- La distribution Ubuntu Core 22 est prête

17 juin 2022

Dans "Développement"
- Ubuntu 20.10 est disponible: voici ce qui change

23 octobre 2020

Dans "Applications"

← Article précédent

Article suivant →

Must Read

ideXlab lance sa nouvelle plateforme d’intermédiation

Applications



SUSE Linux Enterprise Server 12 pour les applications SAP

Applications

GoodTech.info

Home
Applications
Tribunes & Opinions
^renda
ériel

L’écosystème GoodTech

LINAGORA
Emploi
OSSA
Twake Workplace

GOODTECH.info est un site web d’actualité sur les technologies éthiques, l’open source et les logiciels libres. Lancé en version le 26 juin 2023, il a succédé à Toolinux (2000-2023). [Nous contacter.](#)

