Veille technologique : Cybersécurité en entreprise

Simon PRINCE

Dans cette veille technologique, nous allons parler d'une faille de sécurité dans **le noyau Linux d'Ubuntu** et comment faire pour pouvoir régler cette faille de sécurité.

Cette faille de sécurité a été annoncée par un bulletin de sécurité publié par Ubuntu et relayer par CVE et CERT-FR. Cette faille concerne une fuite de mémoire dans le noyau de Linux. Un attaquant pourrait utiliser cette vulnérabilité pour provoquer **un plantage du système** ou éventuellement **exécuter du code arbitraire**. C'est une faille de type « use-after-free ». Cette faille concerne aussi **le noyau Linux de RedHat**.

Pour régler cette faille de sécurité, il suffit de mettre à jour le système. Cette faille a été régler dans **la version 102.1** du noyau de Linux d'Ubuntu. Si vous souhaitez vérifier la version de votre noyau, vous pouvez effectuer la commande : *canonical-livepatch status*

Sources :

https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0275/

https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0277/

https://ubuntu.com/security/notices/LSN-0102-1

https://www.cve.org/CVERecord?id=CVE-2024-1086