



BULLETIN DE SECURITE

Titre	Zero-day dans Linux Kernel
Numéro de Référence	54692305/25
Date de Publication	23 Mai 2025
Risque	Critique
Impact	Critique

Systemes affectés

- Linux kernel version 6.12.27
- Linux kernel version 6.14.5
- Linux kernel version 6.15-rc4

Identificateurs externes

- CVE-2025-37899

Bilan de la vulnérabilité

Une vulnérabilité critique de type zero-day a été identifiée dans le composant ksmbd du noyau Linux. Cette faille peut permettre à un attaquant d'exécuter du code arbitraire à distance avec des privilèges noyau.

Solution

Veuillez se référer aux bulletins de sécurité de différentes distributions Unix pour plus d'information.

Risque

- Exécution du code arbitraire à distance
- Elévation de privilèges

Annexe

- Kernel :
- <https://git.kernel.org/stable/c/02d16046cd11a5c037b28c12ffb818c56dd3ef43>
- <https://git.kernel.org/stable/c/2fc9feff45d92a92cd5f96487655d5be23fb7e2b>
- <https://git.kernel.org/stable/c/d5ec1d79509b3ee01de02c236f096bc050221b7f>
- debian:
- <https://security-tracker.debian.org/tracker/CVE-2025-37899>
- SUSE:openSUSE-SU-2020:1655 :
- <https://www.suse.com/fr-fr/security/cve/CVE-2025-37899.html>
- Ubuntu:
- <https://ubuntu.com/security/CVE-2025-37899>