



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans KSMBD
<b>Numéro de Référence</b>	52232901/25
<b>Date de Publication</b>	29 Janvier 2025
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- Linux kernel 5.15 et versions antérieures

### Identificateurs externes

- CVE-2024-56626, CVE-2024-56627

### Bilan de la vulnérabilité

Deux vulnérabilités critiques ont été corrigées dans KSMBD, le serveur SMB intégré au noyau de Linux. L'exploitation réussie de ces vulnérabilités pourrait permettre à un attaquant d'exécuter du code arbitraire à distance, de porter atteinte aux informations confidentielles et de prendre le contrôle de systèmes vulnérables.

### Solution

Veuillez se référer au bulletin de sécurité afin d'installer les nouvelles mises à jour.

### Risque

- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données
- Prise de contrôle du système affecté

### Référence

Bulletin de sécurité:

- <https://git.kernel.org/stable/c/27de4295522e9a33e4a3fc72f7b8193df9eebe41>
- <https://git.kernel.org/stable/c/6bd1bf0e8c42f10a9a9679a4c103a9032d30594d>

- <https://git.kernel.org/stable/c/81eed631935f2c52cdaf6691c6d48e0b06e8ad73>
- <https://git.kernel.org/stable/c/de4d790dcf53be41736239d7ee63849a16ff5d10>
- <https://git.kernel.org/stable/c/fc342cf86e2dc4d2edb0fc2ff5e28b6c7845adb9>
- <https://git.kernel.org/stable/c/164d3597d26d9acff5d5b8bc3208bdcca942dd6a>
- <https://git.kernel.org/stable/c/1aea5c9470be2c7129704fb1b9562b1e3e0576f8>
- <https://git.kernel.org/stable/c/313dab082289e460391c82d855430ec8a28ddf81>
- <https://git.kernel.org/stable/c/8cd7490fc0f268883e86e840cda5311257af69ca>
- <https://git.kernel.org/stable/c/c5797f195c67132d061d29c57a7c6d30530686f0>