Sommaire

Un défaut de gestion de la mémoire de la fonctionnalité *chroot* dans Sudo permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire sur le système.

Shinken Entreprise non Impacté

Nous décrivons cette faille pour **éviter** que vous vous inquiétiez sur votre installation de **Shinken actuelle**.

Les détails des impacts la faille de Sudo sont dans https://access.redhat.com/security/cve/cve-2023-27320

En résumé:

- Il y a une faille dans les versions très récentes de sudo: un attaquant peux tenter de contourner la fonctionnalité "chroot" pour prendre localement le contrôle du système
- IMPORTANT: ceci touche uniquement les Sudo >= 1.9.8, ce qui signifie:
  - Centos/RedHat 6: **NON IMPACTE**
  - Centos/RedHat 7: **NON IMPACTE**
  - Centos/RedHat 8: **NON IMPACTE**
  - Centos/RedHat 9: **NON IMPACTE**

Pas d'impact pour Shinken Enterprise

Ceci signifie qu'en date de Mars 2023, les systèmes **Shinken Enterprise** ne sont **PAS** impactés