

Faillles de sécurité (CVE)

Objectif

Vous trouverez ci-dessus la liste des pages qui décrivent les failles que nous avons identifiées comme potentiellement à risque pour une installation Shinken :

- Soit elles nécessitent une intervention pour les corriger
- Soit elles sont suffisamment populaires pour vous inquiéter, mais elle ne concerne pas Shinken.

Il s'agit d'une liste la plus à jour suivant notre expérience, que nous maintenons au fil du temps.



Ne pas hésiter à nous suggérer l'analyse de CVE qui ne serait pas dans cette liste

Dans le but d'être le plus à jour et de prendre le moins de risque :

- n'hésitez pas de nous poser des questions sur le sujet,
- ou de nous signaler des failles qui ne seraient indiquées comme traitées.

- [CVE-2023-27320](#) : Faille de sudo dans les versions >= 1.9.8 (RedHat/Centos non impactés)
- [CVE-2022-3786](#) & [CVE-2022-3602](#) : Faille des certificats de sécurités sur OpenSSL (RedHat 9 seulement)
- [CVE-2021-44228](#) - Faille log4j n'impacte pas Shinken (2021)
- [CVE-2021-43798](#) - Faille grafana présente en 8.X (2021)
- [CVE-2021-4034](#) - Faille dans le paquet polkit (non installé par défaut) (2022)
- [CVE-2021-3156](#) - Faille sudoedit pour Centos (2021)