

# CVE-2021-3156 - Faille sudoedit pour Centos ( 2021 )

## Sommaire

Description  
Pour détecter que l'on est vulnérable  
Impact et correction de la faille ( Centos7 seulement )

## Description

Les détails de la faille dans la commande sudoedit sont dans <https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit>

En résumé:

- On peut avoir un passage root d'un utilisateur ( *genre shinken* ) si et seulement si, un utilisateur arrive à lancer la commande **sudoedit** avec les bons arguments.

## Pour détecter que l'on est vulnérable

```
$ sudoedit -s /
```

Retour au début de ligne	Vulnérable (ou pas)
"sudoedit:"	<b>VULNERABLE</b>
"usage:"	<b>FIXE</b>

## Impact et correction de la faille ( Centos7 seulement )

- Dans le cadre de Shinken Enterprise, nous utilisons la commande **sudo** mais **PAS** la commande affectée nommée **sudoedit**.
- Ainsi, la seule possibilité d'exploitation est dans le fait qu'un shinken admin ( **PAS** un admin SI ) peut définir une commande avec **sudoedit** et la faire lancer sur:
  - le Synchronizer
  - les Pollers
  - et ainsi passer root s'il a un bon payload de piratage
- sudo n'est **PAS** livré dans Shinken Enterprise, car il est inclus dans le système
- Les clients **DOIVENT** mettre à jour via la commande :

```
◦ yum install -y sudo
```



**IMPORTANT: Centos6 n'est PAS fixé**

**Remarque:** en Centos6, vu que le système n'est plus supporté, il n'y a pas de correction, il FAUT passer ses serveurs en Centos7