# Baron Samedit : à double faille dans Sudo, doubles dégâts ?

Il aura fallu près de dix ans pour qu'on découvre Baron Samedit. Qualys* a donné ce nom à une vulnérabilité (CVE-2021-3156) qui touche Sudo, utilitaire standard sur les systèmes Unix et Linux pour exécuter des commandes avec les droits d'administration.

On aura reconnu l'allusion à Baron Samedi. Mais pourquoi avec un t ? Parce que la vulnérabilité implique la commande sudoedit, destinée à éditer des fichiers. On l'utilise en l'occurrence pour activer une autre faille, présente dans l'exécution de Sudo en mode shell (option -i ou -s).

Dans les grandes lignes, le problème tient à la gestion de la barre oblique inversée qui sert de caractère d'échappement. Exécuté en mode shell, Sudo en accole une à tous les caractères spéciaux dans les arguments de la ligne de commande.
La politique de sécurité sudoers inclut du code qui concatène l'ensemble en un tampon « user_args ». Et supprime les caractères d'échappement, notamment à des fins de journalisation. Le souci se pose si un argument se termine par une barre oblique seule. On entre alors dans une boucle qui mène au dépassement du tampon.

## Sudo : deux failles n'en font qu'une

Normalement, ce cas ne se présente pas. Mais on peut le forcer en exécutant sudoedit… avec l'option -s ou -i. Cela permet de conserver la faille du mode shell. Tout en empêchant Sudo de doubler les barres obliques dans les arguments.

Baron Samedit était apparu à l'été 2011 avec Sudo 1.8.2. Toutes les versions ultérieures sont touchées dans leur configuration par défaut. Conséquence potentielle : l'obtention de privilèges d'administration par tout utilisateur local, authentifié ou non et présent ou non dans le fichier sudoers.

La solution ? Mettre à jour Sudo (au moins en version 1.9.5p2+) ou les distributions Linux qui l'embarquent (les principales ont appliqué le correctif).

** Qualys propose un modèle de dashboard à utiliser sur sa plate-forme cloud pour évaluer la présence de Baron Samedit. Il est illustré ci-dessous.*

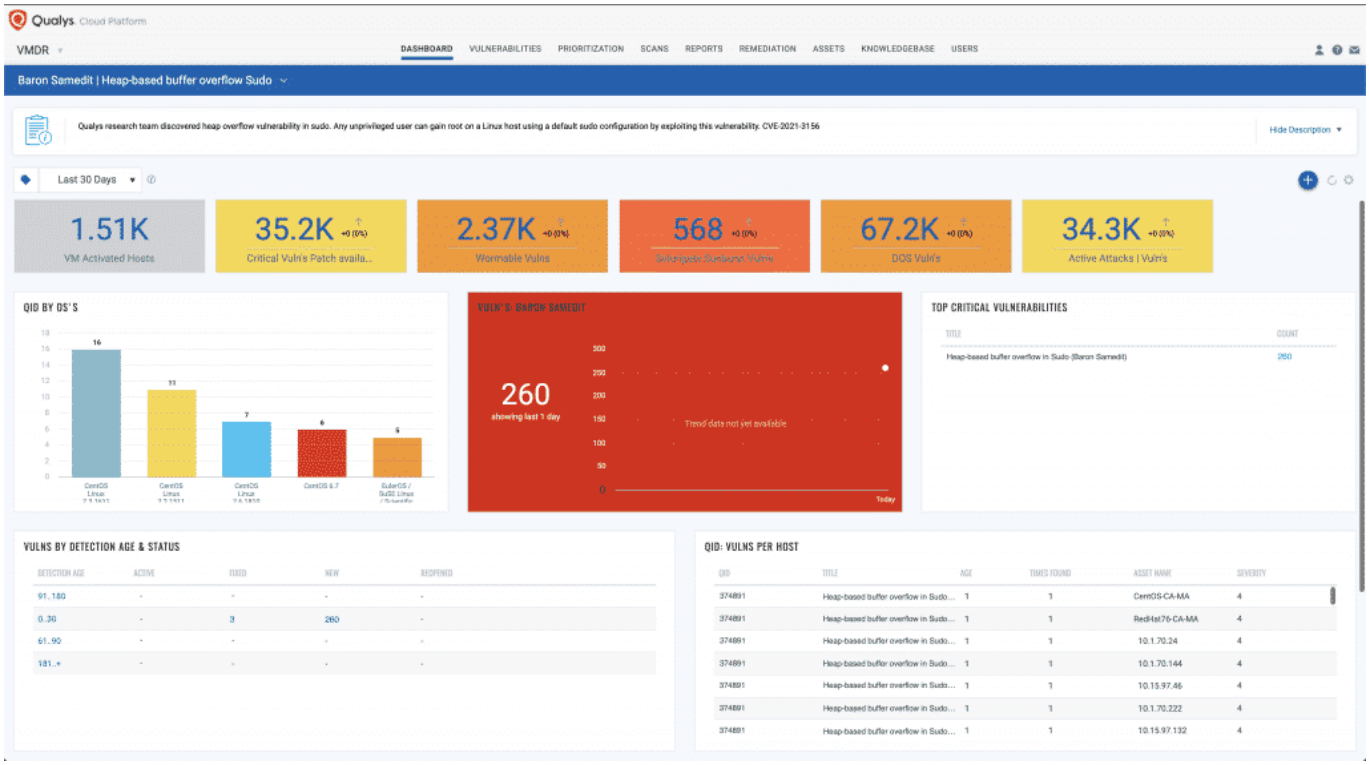


*Illustration principale © swvist / CC BY-SA 2.0*