Forum: Sécurité

Topic: Faille de sécurité critique du registre Windows

Subject: Faille de sécurité critique du registre Windows

Publié par: Lotesdelere
Contribution le : 22/07/2021 23:37:23

Une faille critique de Windows 10 et 11 nommée CVE-2021-36934, ou plus familèrement SeriousSAM ou HiveNightmare, permet d'accéder dans certains cas aux ruches (hive) du registre SAM, SECURITY et SYSTEM et par voie de conséquence à l'ensemble du système. Outre les paramètres contenus dans SYSTEM, la ruche SAM (Security Account Manager) contient tous les mots de passe des différents utilisateurs d'un système Windows, les mots de passe des utilisateurs administratifs inclus.
Il semble que le problème vienne de la mise à jour KB5004605 et est plus généralement présent sur toutes les versions de Windows 10 à partir de la version 1809, et donc toutes les versions actuellement existantes de WIndows 11.

En attendant un correctif, Microsoft conseille d'appliquer les mesures suivantes:
https://msrc.microsoft.com/update-guid ... nerability/CVE-2021-36934

Réduire la possibilité d'accès à %windir%system32config :
Lancer une Invite de commandes ou PowerShell en tant qu'administrateur,
Et y exécutez la commande suivante: icacls %windir%system32config*.* /inheritance:e

Puis il faut supprimer les clichés instantanés du Volume Shadow Copy Service (VSS):
Lancer une Invite de commandes ou PowerShell en tant qu'administrateur,
Exécutez y la commande: vssadmin list shadows (affiche tous les clichés instantanés existants d'un volume spécifié),
S'il y en a, supprimez-les avec: vssadmin delete shadows /for=c : /Quiet
Exécutez à nouveau la commande: vssadmin list shadows (pour vérifier que le suppression a bien été effective),
Puis supprimez tous les points de restauration du système qui existaient avant la restriction de l'accès à %windir%system32config.
Créez éventuellement un nouveau point de restauration du système.

Source (en anglais):
https://www.neowin.net/news/microsoft- ... ffects-windows-10-and-11/