Samba victime d'une faille critique : quelles options ?

Avez-vous bien mis Samba à jour ? Des correctifs ont été publiés cette semaine. Ils éliminent trois failles, dont une critique (9,9/10). Immatriculée CVE-2021-44142, elle repose sur un module VFS : fruit.

Ce module renforce la compatibilité avec les clients macOS et l'interopérabilité avec les serveurs Netatalk. C'est dans sa configuration par défaut qu'il pose problème. Le risque : l'exécution de code à distance. Y compris par des utilisateurs non authentifiés, voire des invités. Il leur suffit d'avoir un accès en écriture aux attributs étendus des fichiers ouverts dans le démon smbd.

En cas d'impossibilité d'installer le patch (versions 4.13.17, 4.14.2 et 4.15.5), il existe une méthode de contournement : retirer le module fruit de toutes les lignes « vfs objects » dans la configuration de Samba.
La vulnérabilité ne peut s'enclencher si on modifie les options fruit:metadata=netatalk et fruit:resource. Mais procéder ainsi rend les données stockées inaccessibles aux clients macOS, qui les croient perdues.

Autre faille au score de criticité élevé : CVE-2022-0336. Elle peut permettre aux utilisateurs Active Directory d'usurper l'identité de services. Ce en modifiant les attributs SPN (servicePrincipalName).

La troisième faille (CVE-2021-44141) est moins critique : 4,2/10. Elle peut permettre, au travers des liens symboliques, de déterminer si des fichiers ou des dossiers existent sur le serveur, hors d'un partage Samba.

Photo d'illustration © Brian A Jackson – Shutterstock