Nadir DJEDIDEN
Nassim BENBOUHAMOU
Ismael BAHRI

20/12/2023

VEILLE INFORMATIONNELLE

DJEDIDEN Nadir
[NOM DE LA SOCIETE]

PLAN :

II. CVE TrueNas

CVE-2022-23122 : netatalk - setfilparams Exécution de code à distance par dépassement de tampon basé sur la pile

Versions concernées : toutes les versions antérieures à TrueNAS Core 12.0-U8.1 Pour vérifier si un système est vulnérable, exécutez afpd -v. Les systèmes dont la chaîne de version n'est pas 3.1.13 ou plus récente sont vulnérables.

Description :

Cette vulnérabilité permet à des attaquants distants de divulguer des informations sensibles sur les installations affectées de Netatalk. L'authentification n'est pas requise pour exploiter cette vulnérabilité.

La faille spécifique existe dans la fonction setfilparams. Le problème résulte du manque de validation appropriée de la longueur des données fournies par l'utilisateur avant de les copier dans un tampon basé sur une pile de longueur fixe. Un attaquant peut exploiter cette vulnérabilité pour exécuter du code dans le contexte de root.

Aucune solution de contournement n’est possible, il faut attendre la mise à jour pour réparer cette vulnérabilité.

Mais afin d’atténuer les risques, il est possible de désactiver les partages AFP concernés jusqu’à ce que la mise à jour soit disponible.

Dans le TrueNAS 12.0-U8.1 cette vulnérabilité est corrigé.

Lien vers la CVE : https://security.truenas.com/cves/2022-03-21-cve-2022-23122/