

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 31-03-2024

BULLETIN ALERTES

Object	Vulnérabilité dans SSH
Référence	1131
Date de Publication	2024-03-30
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Accès non autorisé.

SYSTÈME AFFECTÉ :

- Tous les versions base sur linux utilisant la bibliothèque liblzma

DÉSCRIPTION :

Du code malveillant a été découvert dans les archives tar sources de xz, à partir de la version 5.6.0. Grâce à une série de techniques d'obscurcissement complexes, le processus de construction de liblzma extrait un fichier objet précompilé à partir d'un fichier de test déguisé présent dans le code source. Ce fichier objet est ensuite utilisé pour modifier des fonctions spécifiques du code liblzma. Cela aboutit à une librairie liblzma modifiée qui peut être utilisée par tout logiciel lié à cette librairie, interceptant et modifiant l'interaction des données avec cette dernière.

CONTOURNEMENT PROVISOIRE :

Fermeture de tout accès SSH aux équipements exposés.

DOCUMENTATION :

- Bulletin de sécurité Redhat
https://bugzilla.redhat.com/show_bug.cgi?id=2272210
- Bulletin de sécurité OpenWall
<https://www.openwall.com/lists/oss-security/2024/03/29/4>
- CVE-2024-3094
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-3094>