ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	« Supply chain » attaque contre XZ Utils
Numéro de Référence	46810104/24
Date de Publication	01 Avril 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- XZ Utils versions 5.6.0 et 5.6.1

Identificateurs externes

- CVE-2024-3094

Bilan de la vulnérabilité

Des chercheurs en sécurité ont révélé une vulnérabilité critique (CVE-2024-3094) dans XZ Utils utilisé dans les distributions Linux. XZ Utils est victime d'une « Supply Chain » attaque La vulnérabilité a un score CVSSv3 (Common Vulnerability Scoring System) de 10 sur 10.

Un code malveillant a été intégré dans les versions 5.6.0 et 5.6.1 de XZ Utils. L'exploitation réussie de la vulnérabilité pourrait permettre à un attaquant non autorisé de contourner l'authentification sshd et d'obtenir un accès à distance à l'ensemble du système.

Les utilisateurs des distributions Linux sont invités à vérifier si leurs systèmes utilisent les versions XZ concernées en entrant « xz –version » dans la ligne de commande. Si leur système utilise une version affectée, les utilisateurs sont invités à passer à la version 5.4.x de XZ ou à désactiver immédiatement les services SSH, et à vérifier que leur système ne présente pas d'activité malveillante ou suspecte.

Solution

Veuillez se référer aux bulletins de sécurité pour plus d'information.

Risque

- Prise de contrôle du système affecté
- Contournement d'authentification

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Annexe

Bulletin de sécurité :

- https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users
- https://sec.cloudapps.cisco.com/security/center/publicationListing.x
- https://news.opensuse.org/2024/03/29/xz-backdoor/
- https://lists.debian.org/debian-security-announce/2024/msg00057.html
- https://www.openwall.com/lists/oss-security/2024/03/29/4