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	Vulnérabilité critique dans noyau Linux
Numéro de Référence	55322006/25
Date de Publication	20 Juin 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Tous les systèmes Linux dont le noyau est inférieur à la version 6.2

Identificateurs externes

- CVE-2023-0386

Bilan de la vulnérabilité

Une vulnérabilité critique « CVE-2023-0386 » affecte le sous-système « OverlayFS » du noyau Linux. Le noyau ne vérifie pas correctement si l'UID/GID du fichier copié depuis « OverlayFS » vers le "upper" est mappé dans l'espace utilisateur courant, permettant à un utilisateur non privilégié de créer un binaire « SUID root » dans un répertoire comme "/tmp", et de l'exécuter pour obtenir les privilèges « root ».

Des preuves de concept (PoC) sont publiquement disponibles, il est fortement recommandé d'appliquer les correctifs de sécurité proposés par les distributions linux concernées (Ubuntu, Red Hat, Debian…).

Solution :

Veuillez se référer aux bulletins de sécurité des distributions linux concernées pour plus d'infirmation.

Risque :

- Prise de contrôle complète du système par un utilisateur local non privilégié
- Exécution de commandes ou de programmes avec les droits root

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

- Elévation de privilèges

Annexe

Bulletin de sécurité Ubuntu **:**

- https://ubuntu.com/security/CVE-2023-0386

Bulletin de sécurité Debian**:**

- https://security-tracker.debian.org/tracker/CVE-2023-0386

Bulletin de sécurité Amazon Linux**:**

- https://explore.alas.aws.amazon.com/CVE-2023-0386.html

Bulletin de sécurité RedHat**:**

- https://access.redhat.com/security/cve/cve-2023-0386