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 les produits Cisco
Numéro de Référence	48110407/24
Date de Publication	04 juillet 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Cyber Vision
- Prime Infrastructure
- Cisco Meeting Server
- Expressway Series
- TelePresence Video Communication Server (VCS)
- IEC6400 Edge Compute Appliance

Identificateurs externes

- CVE-2024-6387

Bilan de la vulnérabilité

Une vulnérabilité critique a été corrigée dans les produits Cisco susmentionnés utilisant des versions vulnérables de OpenSSH. Cette vulnérabilité permet à un attaquant non authentifié d'exécuter du code arbitraire à distance avec les privilèges root. Un attaquant pourrait exploiter cette faille afin de contrôler le système affecté.

Solution

Veuillez se référer au bulletin de sécurité Cisco 03 juillet 2024 pour plus d'information.

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

Risque

- Contrôle du système affecté
- Exécution du code arbitraire à distance
- Elévation de privilèges

Annexe

Bulletin de sécurité Cisco 03 juillet 2024:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssh-rce-2024