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

NOTE D'INFORMATION

Titre	« Supply chain » attaque contre Codecov
Numéro de Référence	30070305/21
Date de Publication	03 Mai 2021
Risque	Critique
Impact	Critique

Codecov est victime d'une « Supply Chain » attaque. Pendant plus de deux mois, des hackers ont détourné les outils de Codecov pour espionner des centaines d'entreprises. Des hackers sont parvenus à s'introduire sur son système et à modifier, à plusieurs reprises, un de ses scripts, nommé « Bash Uploader », qu'elle utilise dans plusieurs de ses outils. Le malware inséré dans le code permettait aux attaquants de détecter et d'intercepter toutes sortes d'informations confidentielles comme des identifiants, des jetons d'authentification ou des clés de chiffrement.

Après la vaste opération de cyber-espionnage permise par l'attaque contre Solarwinds, cette nouvelle attaque à la « Supply Chain » logicielle pourrait avoir compromis les systèmes d'un grand nombre d'entreprises.

Recommandation :

Codecov a publié des indicateurs de compromission (IOC) et un ensemble de données non exhaustif de variables d'environnement probablement compromises, pour aider les organisations à déterminer si elles ont été affectées.

Les utilisateurs concernés doivent immédiatement mettre en œuvre les conseils figurant dans les sections « Actions recommandées aux utilisateurs concernés et FAQ » de la note d'information de Codecov. Il est recommandé d'accorder une attention particulière aux conseils de Codecov sur le changement ("re-rolling") des informations d'identification, des jetons et des clés potentiellement affectés. Il est également recommandé de révoquer et de réémettre tout certificat potentiellement affecté.

Référence :

Note d'information de sécurité Codecov du 29 Avril 2021:

- https://about.codecov.io/security-update/

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