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 DE SECURITE

Titre	« Supply chain attaque » Compromission de RVTools
Numéro de Référence	54602005/25
Date de Publication	20 Mai 2025
Risque	Critique
Impact	Critique

Le 13 mai 2025, des chercheurs en sécurité ont détecté une compromission de « RVTools » dans une attaque de chaîne d'approvisionnement. Des utilisateurs ont téléchargé une version corrompue de RVTools, un outil légitime de gestion VMware, contenant un fichier malveillant (version.dll) détecté comme une variante du Malware « Bumblebee ». Les métadonnées suspectes et la divergence des signatures des fichiers (hash) ont confirmé la compromission, probablement due à un piratage temporaire du site officiel.

Après une réaction rapide, RVTools a rétabli une version propre. Les utilisateurs ayant récemment installé RVTools sont invités à vérifier l'intégrité de leur version et à rechercher toute exécution suspecte de version.dll.

Indicateurs de compromission (IOCs):

Hash:

- version.dll : 27282e66e73fb247ba92a91f500b52d641549a8388e35155938b0d2da3abd537

Annexe

Bulletin de sécurité :

- https://zerodaylabs.net/rvtools-bumblebee-malware/

VirusTotal : version malveillante du RVTools:

- https://www.virustotal.com/gui/file/27282e66e73fb247ba92a91f500b52d641549a8388e35155938b0d2da3abd537/community

VirusTotal : version propre du RVTools:

- https://www.virustotal.com/gui/file/0506126bcbc4641d41c138e88d9ea9f10fb65f1eeab3bff90ad25330108b324c/detection

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