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	Zero-day dans la solution de vidéoconférence ZOOM
Numéro de Référence	24090304/20
Risque	Critique
Impact	Critique

Systèmes affectés

- ZOOM

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été découvertes dans la solution de vidéoconférence ZOOM. Parmi ces vulnérabilités, un Zero-Day qui permet à un attaquant de voler les informations d'identification et d'authentification de Windows à l'aide d'un lien malveillant envoyé à un utilisateur exécutant ZOOM sur sa machine. Une fois l'utilisateur clique sur ce lien malveillant, Windows envoi le nom de connexion de l'utilisateur et le hash du mot de passe NTLM, qui peut être décrypté facilement. En plus, l'exploitation de cette faille peut permettre à un attaquant d'exécuter des commandes à distance.

Solution :

Les utilisateurs manipulant des informations sensibles doivent arrêter l'utilisation de cette solution et de procéder au changement de leurs mots de passes d'authentification Windows.

Risque :

- Accès aux informations confidentielles ;
- Exécution de commande arbitraire à distance ;

Références :

- https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/
- https://www.cyberscoop.com/zoom-zero-day-webcam-privlege-escalation/

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma