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	« TunnelVision » Vulnérabilité du contournement du VPN
Numéro de Référence	47381305/24
Date de Publication	13 Mai 2024
Risque	Critique
Impact	Critique

Une nouvelle technique, appelée « TunnelVision », a été récemment découverte, qui peut contourner l'encapsulation VPN et permettre aux attaquants d'envoyer le trafic hors d'un tunnel VPN en utilisant les fonctionnalités intégrées du Dynamic Host Configuration Protocol. (DHCP). TunnelVision permet le routage du trafic sans cryptage via un VPN. Ce trafic peut être dirigé par le serveur DHCP configuré par l'attaquant à l'aide de l'option 121, pour finalement être redirigé vers Internet via un canal secondaire créé par l'attaquant. Le tunnel VPN existant reste intact et le canal secondaire créé par l'attaquant ne peut pas être détecté par le tunnel VPN existant. CVE-2024-3661 a été attribué à cette vulnérabilité critique.

Recommandation :

- Veiller à ce que le système d'exploitation, le client VPN et les autres logiciels soient mis à jour avec les derniers correctifs de sécurité.
- Si possible, ignorez l'option 121 pour le serveur DHCP lorsque le réseau VPN est utilisé.
- Mettre en œuvre le snooping DHCP sur les switch de réseau afin d'empêcher les serveurs DHCP non autorisés.
- Activer la protection ARP pour empêcher l'usurpation du protocole de résolution d'adresses (ARP).
- Utiliser un service VPN réputé, avec une solide expérience en matière de sécurité.

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

Référence :

TunnelVision**:**

- https://thehackernews.com/2024/05/new-tunnelvision-attack-allows.html
- https://www.helpnetsecurity.com/2024/05/08/tunnelvision-cve-2024-3661/

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