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	Incident de sécurité affectant le service Cloud Backup de SonicWall
Numéro de Référence	57391310/25
Date de Publication	13 Octobre 2025
Risque	Critique
Impact	Critique

Suite à l'incident de sécurité lié au service « Cloud Backup » de SonicWall qui a fait l'objet de la note de sécurité « 56982309/25 » de la DGSSI, La firme de sécurité « Huntress » a observé une compromission massive de dispositifs SonicWall SSLVPN chez plusieurs de ses clients.

Cette compromission consiste en des authentifications réussies à grande échelle, ce qui laisse penser que les attaquants disposaient d'identifiants valides.

Huntress signale que l'activité suspecte est antérieure à mi-septembre (date de l'incident affectant le service Cloud Backup) et qu'ils ne peuvent pas assurer qu'elle soit directement liée à l'incident de sauvegarde Cloud.

La DGSSI recommande à l'ensemble des utilisateurs de vérifier si leurs équipements sont concernés par cet incident, le cas échéant, de :

- Restreindre ou désactiver l'accès WAN (gestion distante, VPN)
- Réinitialiser tous les identifiants d'administration
- Renouveler les clés VPN (pre-shared keys), certificats
- Révoquer et recréer les clés d'API, comptes externes connectés au pare-feu
- Activer l'authentification multi-facteur (MFA) partout où c'est possible

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

Annexe

Bulletin de sécurité SonicWall :

- https://www.sonicwall.com/support/knowledge-base/mysonicwall-cloud-backup-file-incident/250915160910330

Note de sécurité de « Huntress » :

- https://www.huntress.com/blog/sonicwall-sslvpn-compromise