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	Vulnérabilité critique dans Barracuda Email Security Gateway
Numéro de Référence	45342812/23
Date de Publication	28 Décembre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Barracuda Email Security Gateway versions 5.1.3.001 à 9.2.1.001

Identificateurs externes

- CVE-2023-7102

Bilan de la vulnérabilité

Une vulnérabilité critique a été corrigée dans Barracuda Email Security Gateway. La vulnérabilité « CVE-2023-7102 » existait dans « Spreadsheet::ParseExcel », une bibliothèque tierce open-source utilisée par le scanner de virus Amavis au sein de l'appliance ESG.

L'exploitation réussie de la vulnérabilité d'exécution de code arbitraire dans Spreadsheet::ParseExcel pourrait permettre à un attaquant distant de déployer des logiciels malveillants notamment (SEASPY et SALTWATER) via des pièces jointes d'email au format Excel spécialement conçues.

Solution :

Veuillez se référer au bulletin de sécurité Barracuda afin d'installer les nouvelles mises à jour.

Risque :

- Exécution des commandes à distance,

Annexe

Bulletin de sécurité Barracuda**:**

- https://www.barracuda.com/company/legal/esg-vulnerability

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