



BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans Barracuda Email Security Gateway
Numéro de Référence	42072505/23
Date de Publication	25 Mai 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Barracuda Email Security Gateway versions 5.1.3.001 à 9.2.0.006

Identificateurs externes

- CVE-2023-2868

Bilan de la vulnérabilité

Une vulnérabilité critique a été corrigée dans Barracuda Email Security Gateway. La vulnérabilité existait dans un module qui filtre initialement les pièces jointes d'e-mails entrants. Un attaquant distant peut exploiter cette faille via l'envoi des pièces jointes malicieuses qui entraînera l'exécution à distance d'une commande système avec les privilèges du produit Email Security Gateway.

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://status.barracuda.com/incidents/34kx82j5n4q9>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2868>