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 Libraesva ESG (Email Security Gateway)
Numéro de Référence	57103009/25
Date de Publication	30 Septembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Libraesva ESG 5.0 version antérieure à 5.0.31
- Libraesva ESG 5.1 version antérieure à 5.1.20
- Libraesva ESG 5.2 version antérieure à 5.2.31
- Libraesva ESG 5.3 version antérieure à 5.3.16
- Libraesva ESG 5.4 version antérieure à 5.4.8
- Libraesva ESG 5.5. version antérieure à 5.5.7

Identificateurs externes

- CVE- 2025-59689

Bilan de la vulnérabilité

Une vulnérabilité critique a été corrigée dans Libraesva ESG (Email Security Gateway). Un attaquant peut exploiter cette faille d'injection de commandes via l'envoi d'un e-mail malveillant contenant une archive compressée spécialement conçue afin d'exécuter des commandes arbitraires avec les droits d'un utilisateur non privilégié, ouvrant la voie à une compromission totale du système.

Solution :

Veuillez se référer aux bulletins de sécurité Libraesva pour plus d'infirmation.

Risque :

- Exécution de commandes arbitraire à distance
- Elévation de privilèges

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

- Compromission de système

Annexe

Bulletin de sécurité Libraesva**:**

- https://docs.libraesva.com/knowledgebase/security-advisory-command-injection-vulnerability-cve-2025-59689/