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	SMTP Smuggling attaque
Numéro de Référence	45420501/24
Date de Publication	05 Janvier 2024
Risque	Critique
Impact	Critique

Une nouvelle technique d'exploitation appelée « Simple Mail Transfer Protocol (SMTP) smuggling » peut être utilisée par des acteurs malveillants pour envoyer des courriels usurpés avec de fausses adresses d'expéditeur tout en contournant les mesures de sécurité.

Ces acteurs peuvent exploiter les serveurs SMTP vulnérables pour envoyer des courriels malveillants à partir d'adresses électroniques arbitraires, ce qui permet des attaques ciblées par hameçonnage, via l'envoi de faux courriels qui semblent provenir d'expéditeurs légitimes et de déjouer les contrôles de sécurité mis en place pour filtrer les messages entrants.

Il est recommandé de se référer aux différents éditeurs pour appliquer les correctifs et les recommandations préconisées. A titre d'exemple:

- Postfix SMTP vulnérabilité identifiée par CVE-2023-51764 (https://www.postfix.org/smtp-smuggling.html)
- Exim SMTP vulnérabilité identifiée par CVE-2023-51766 (https://bugs.exim.org/show_bug.cgi?id=3063)
- SendMail SMTP vulnérabilité identifiée par CVE-2023-51765
- Cisco Secure Email recommendation https://bst.cisco.com/quickview/bug/CSCwh10142
- Zimbra recommandation: https://blog.zimbra.com/2023/12/zimbra-and-smtp-smuggling-attack-on-postfix/

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 :

SMTP Smuggling :

- https://nvd.nist.gov/vuln/detail/CVE-2023-51764
- https://nvd.nist.gov/vuln/detail/CVE-2023-51766
- https://nvd.nist.gov/vuln/detail/CVE-2023-51765
- https://www.postfix.org/smtp-smuggling.html
- https://bugs.exim.org/show_bug.cgi?id=3063