



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/>

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