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	Vulnérabilités critiques dans Exim Mail Transfer Agent ou MTA
Numéro de Référence	44050310/23
Date de Publication	03 Octobre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Exim versions antérieures à 4.96.1 ou 4.97

Identificateurs externes

- CVE-2023-42115, CVE-2023-42114, CVE-2023-42116, CVE-2023-42117, CVE-2023-42118, CVE-2023-42119

Bilan de la vulnérabilité

Exim annonce la correction de trois vulnérabilités critiques de type « zero-day » parmi les six failles découvertes par Zero Day Initiative (ZDI) affectant les versions antérieures à 4.96.1 ou 4.97 de l'agent de transfert de courriels (*Mail Transfer Agent* ou *MTA*) Exim.

- Une vulnérabilité critique (CVE-2023-42115) affectant Exim Mail Transfer Agent (MTA), en raison d'une faiblesse d'écriture hors limites trouvée dans le service SMTP. La vulnérabilité a un score CVSSv3 (Common Vulnerability Scoring System) de 9.8 sur 10. L'exploitation réussie de la vulnérabilité pourrait permettre à un attaquant distant et non authentifié de réaliser une exécution de code à distance (RCE) sur les serveurs vulnérables.

- Les vulnérabilités identifiées CVE-2023-42114 et CVE-2023-42116 ayant respectivement un score *CVSSv3* de 3.7 et 8.1 sont présentes dans le sous-système *SPA/NTLM*. Ce dernier présente une faiblesse dans la validation des entrées utilisateurs lors du traitement des demandes de défis (*challenges*) *NTLM*. L'exploitation réussie de la vulnérabilité pourrait permettre à un attaquant distant de provoquer une atteinte à la confidentialité des données et une exécution de code arbitraire.

Cependant, à la date de publication initiale de cette alerte, l'éditeur ne propose pas de correctif pour les trois vulnérabilités suivantes :

- La vulnérabilité CVE-2023-42117 ayant un score CVSSv3 de 8.1 est liée à la gestion du protocole PROXY. Un manque de validation des données soumises par l'utilisateur peut permettre à un attaquant distant de compromettre l'intégrité des données en mémoire et de tenter une exécution de code arbitraire.

- La vulnérabilité identifiée CVE-2023-42118 a un score CVSSv3 de 7.5. Un attaquant adjacent au réseau peut tenter une exécution de code arbitraire vers les versions affectées de la bibliothèque libspf2 incluse dans Exim.

- La vulnérabilité dont le numéro d'identification est CVE-2023-42119 est référencée avec un score CVSSv3 de 3.1. Elle est due au sous-système de recherches DNS : un manque de validation des données fournies par l'utilisateur peut entraîner une lecture au-delà du tampon alloué. Un attaquant adjacent au réseau peut alors, en conjonction avec d'autres vulnérabilités, tenter une exécution de code arbitraire dans le contexte du compte de service.

Solution

Exim n'a pas encore publié des correctifs pour les trois vulnérabilités CVE-2023-42117, CVE-2023-42118 et CVE-2023-42119. Les mesures de contournement proposées consistent à :

- Pour CVE-2023-42117 : recourir à un relai (*proxy*) de confiance utilisant le protocole PROXY ;
- Pour CVE-2023-42118 : ne pas utiliser de *macro spf* dans les directives de configuration définissant les listes de contrôles d'accès (Access Control Lis*ts* ou *ACL*) ;
- Pour CVE-2023-42119 : utiliser un résolveur DNS digne de confiance qui est capable de valider les données en fonction des types d'enregistrements DNS.

Veuillez se référer au bulletin de sécurité Exim du 02 Octobre 2023 afin d'installer les nouvelles mises à jour.

Risque

- Contournement de la politique de sécurité
- Exécution du code arbitraire à distance
- Divulgation des informations confidentielles

Annexe

Bulletins de sécurité Exim du 02 Octobre 2023:

- https://www.exim.org/static/doc/security/CVE-2023-zdi.txt

Bulletin de sécurité ZDI du 27 septembre 2023 :

- https://www.zerodayinitiative.com/advisories/ZDI-23-1468/
- https://www.zerodayinitiative.com/advisories/ZDI-23-1469/

- https://www.zerodayinitiative.com/advisories/ZDI-23-1470/
- https://www.zerodayinitiative.com/advisories/ZDI-23-1471/
- https://www.zerodayinitiative.com/advisories/ZDI-23-1472/
- https://www.zerodayinitiative.com/advisories/ZDI-23-1473/