AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Faille critique d'authentification dans les serveurs SmarterMail.

Contenu

I. Contexte

Une vulnérabilité critique, identifiée sous la référence **CVE-2026-23760**, met en péril l'intégrité de milliers de serveurs de messagerie SmarterMail. Selon les chercheurs en cybersécurité, plus de 6 000 instances exposées sur Internet seraient vulnérables à des tentatives de piratage automatisées.

Cette faille permet à un attaquant distant de prendre le contrôle total des serveurs sans aucune authentification préalable.

II. Détails techniques et origine de la faille

Cette vulnérabilité réside dans l'API de réinitialisation de mot de passe du logiciel.

- **Vecteur d'attaque :** Le point de terminaison (endpoint) force-reset-password accepte des requêtes anonymes.
- **Mécanisme :** Le système ne vérifie ni le mot de passe actuel, ni la présence d'un jeton (token) de réinitialisation lors d'une demande concernant un compte administrateur.
- **Impact :** Un attaquant n'a besoin que du nom d'utilisateur de l'administrateur pour définir un nouveau mot de passe, entraînant un compromis total de l'instance et permettant l'exécution de code à distance (RCE) sur l'hôte.

III. Historique et exploitation active

Bien qu'un correctif ait été publié par l'éditeur SmarterTools le 15 janvier (build 9511), l'exploitation de la faille a été confirmée dès le 21 janvier.

Exploitation de masse : La firme Huntress a observé des signes d'attaques automatisées à grande échelle.

Données de scan : Si Shadowserver dénombre 6 000 serveurs à risque, le chercheur Yutaka Sejiyama estime ce chiffre à plus de 8 550 instances encore vulnérables.

Précédent : Cette découverte survient seulement deux semaines après une autre faille critique (**CVE-2025-52691**) touchant le même produit.

IV. Comment se prémunir ?

Mise à jour immédiate : Déployer la version **SmarterMail build 9511** ou ultérieure.

Audit des comptes : Vérifier les journaux d'accès pour toute modification suspecte des comptes administrateurs.

Isolement : Si aucune mise à jour n'est possible, déconnecter l'instance d'Internet ou restreindre drastiquement l'accès à l'interface d'administration par un VPN ou une liste blanche d'IP.

V. Conclusion

Néanmoins, pour éviter d'être victime d'un acteur malveillant connu ou non, il est recommandé de prendre les précautions suivantes :

- N'installer que les applications qui vous sont utiles ;
- Se rassurer de la crédibilité d'une application à l'aide des notes et commentaires attribués par les utilisateurs à celle-ci, avant de les installer ;
- Installer les applications depuis le Store officiel de votre Système d'exploitation (Play Store pour Google Android, App Store pour IOS, etc.) ;
- N'accordez que les autorisations utiles à vos applications pour réaliser les fonctions qu'elles sont censées réaliser ;
- Veillez à mettre à jour régulièrement tous vos logiciels, en installant chaque nouveau correctif de sécurité dès sa publication ;
- Choisissez une solution de sécurité (Antivirus) éprouvée dotée de capacités de détection comportementale pour une protection efficace contre les menaces connues et inconnues, notamment les exploitations de vulnérabilités ;
- Armez-vous des règles élémentaires de cyber-hygiène.