Titre

Flood de réinitialisation de mot de passe permettant l'énumération d'utilisateurs et le spam email

---

Résumé

La fonctionnalité de réinitialisation de mot de passe du site concerné présente deux faiblesses :

- elle permet d'identifier les comptes existants (énumération d'utilisateurs)
- elle ne limite pas le nombre de requêtes, ce qui rend possible l'envoi massif d'emails

Un attaquant peut ainsi vérifier si une adresse est enregistrée, puis déclencher un grand nombre d'emails de réinitialisation, provoquant un spam important, voire une saturation de la boîte de réception ciblée.

Description détaillée Énumération d'utilisateurs

Le comportement de l'application varie selon que l'adresse email est associée ou non à un compte.

- Si l'email n'existe pas :

« L'adresse e-mail que vous avez saisie n'est pas liée à un compte actif. »

- Si l'email est valide :
  → un email de réinitialisation est envoyé sans message d'erreur équivalent

Cette différence permet de déterminer facilement si une adresse est enregistrée sur la plateforme.

Flood de réinitialisation de mot de passe

L'endpoint de réinitialisation ne semble pas intégrer de mécanisme de protection (rate limiting, CAPTCHA, etc.).

Il est possible de :

- soumettre plusieurs requêtes en quelques secondes
- déclencher autant d'emails de réinitialisation sans restriction

Conséquences possibles :

- réception massive d'emails pour la victime
- dégradation de l'expérience utilisateur
- risque de blocage des emails légitimes par les fournisseurs de messagerie

---

Étapes de reproduction

Énumération d'utilisateurs

1. Accéder à la page de connexion du site
2. Cliquer sur « Mot de passe oublié »
3. Tester avec une adresse aléatoire → message d'erreur explicite (L'adresse e-mail que vous avez saisie n'est pas liée à un compte actif.)
4. Tester avec une adresse valide → comportement différent (email envoyé)

Flood d'emails

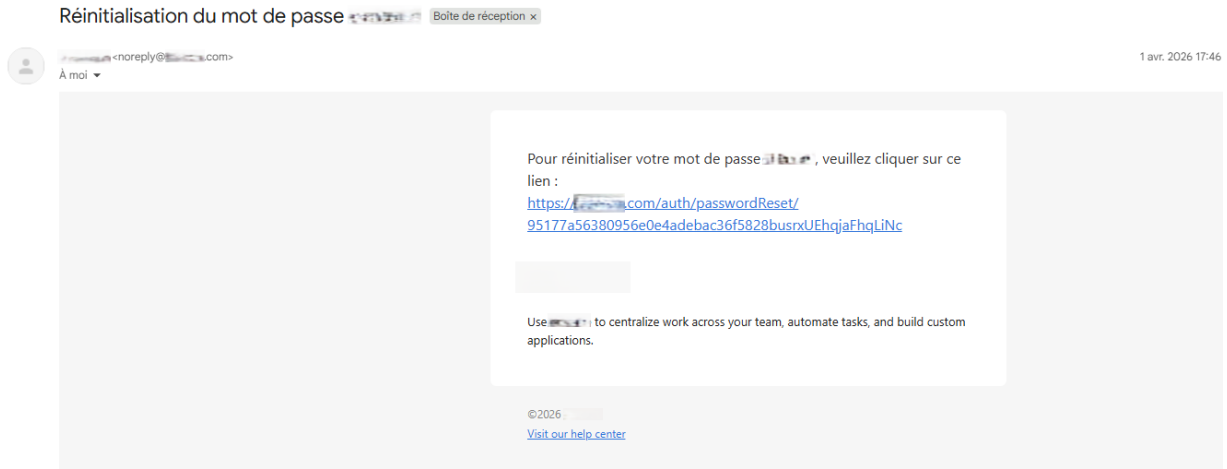
1. Aller sur « Mot de passe oublié »
2. Saisir une adresse email valide (par exemple la vôtre)
3. Cliquer plusieurs fois rapidement sur le bouton d'envoi
4. Vérifier la boîte de réception

→ plusieurs emails sont reçus en quelques secondes

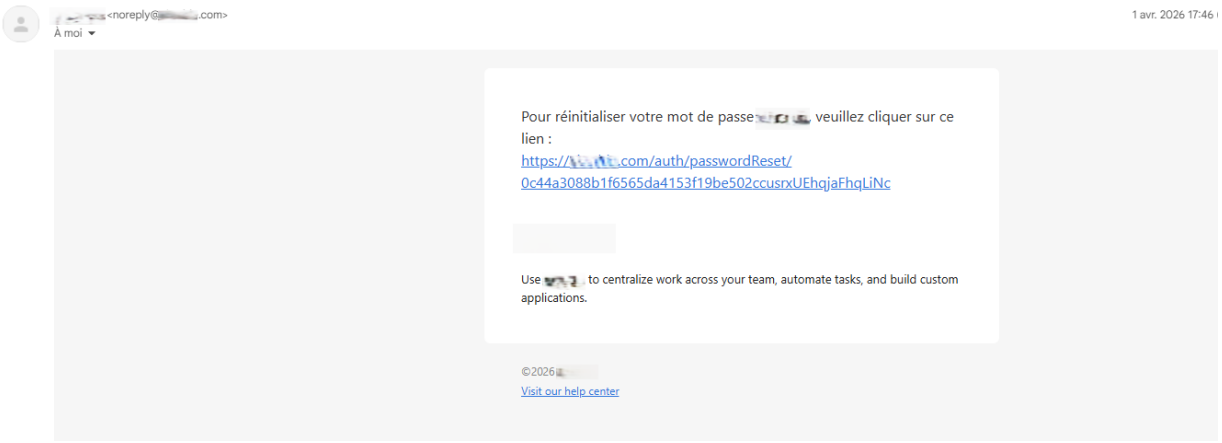
Preuve de concept

Observation de plusieurs emails de réinitialisation reçus quasi instantanément :

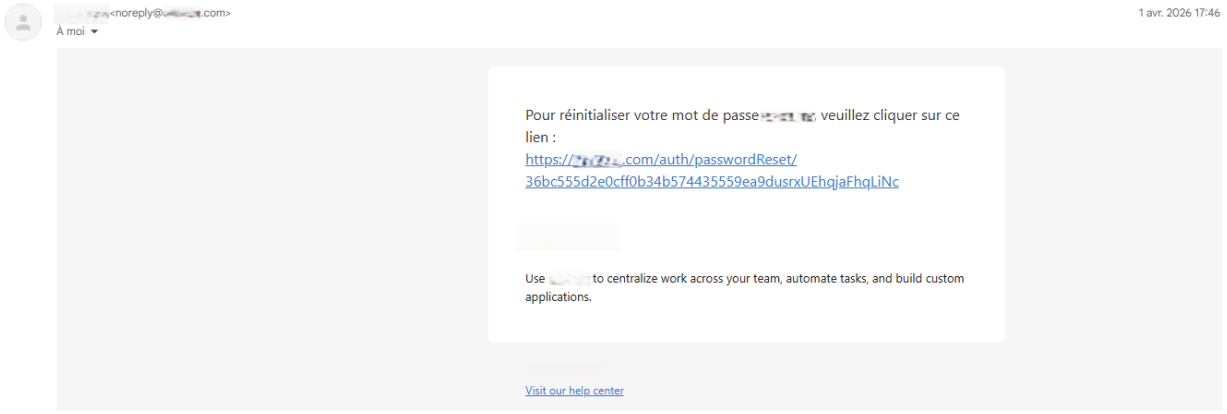
- Email 1 →



- Email 2 →



- Email 3 →



Chaque message contient un lien de réinitialisation fonctionnel.

Impact

- Identification des comptes existants
- Spam ciblé / nuisance utilisateur
- Risque de saturation de boîte mail (DoS léger)
- Facilitation de campagnes de phishing
- Dégradation de la délivrabilité des emails légitimes

Recommandations

- Uniformiser les réponses côté serveur (ne pas révéler si un compte existe)
- Mettre en place un rate limiting sur cet endpoint
- Ajouter un CAPTCHA après plusieurs tentatives
- Implémenter un délai minimal entre deux demandes de réinitialisation

- Envisager une limitation côté utilisateur et côté IP

Sévérité

Moyenne

Remarques

La vulnérabilité est facilement reproductible sans privilèges particuliers, à partir d’un simple compte utilisateur.