

Qu'est-ce qu'un jeton d'actualisation, et pourquoi sa perte est-elle particulièrement dommageable ?

Réponse courte : un jeton d'actualisation (refresh token) est un identifiant de longue durée utilisé pour obtenir silencieusement de nouveaux jetons d'accès sans que l'utilisateur ait à se reconnecter. C'est ce sur quoi repose la fonction « se souvenir de moi ». Comme il peut permettre de générer indéfiniment de nouveaux accès, un jeton d'actualisation dérobé peut offrir à un attaquant un accès durable bien après la fin de votre session.

Jeton d'accès vs. jeton d'actualisation

- **Jeton d'accès (jeton de session) :** de courte durée, utilisé à chaque requête, expire en quelques minutes ou quelques heures.
- **Jeton d'actualisation :** de longue durée, utilisé uniquement pour demander de nouveaux jetons d'accès. Parfois valable pendant des semaines ou des mois.

Un jeton d'accès dérobé finit par expirer. Un jeton d'actualisation dérobé peut être utilisé pour générer de nouveaux jetons d'accès de manière répétée — ce qui transforme un vol ponctuel en un accès persistant.

Pourquoi « se souvenir de moi » implique un compromis

Rester connecté nécessite de stocker un élément durable sur l'appareil. Cette commodité est précisément ce qui rend le jeton stocké précieux pour un attaquant. Les magasins d'identifiants des navigateurs et des applications constituent des emplacements standards et prévisibles, de sorte que les outils automatisés s'y attaquent directement.

Réduire les dommages

Révoquer un jeton d'actualisation invalide l'accès qu'il peut générer — c'est pourquoi la fonction « se déconnecter de tous les appareils » et la révocation des jetons sont importantes après toute compromission suspectée. Mais la révocation est une réponse mise en œuvre *après* le vol.

L'approche de Cyber Crucible consiste à empêcher la lecture. Le magasin d'identifiants est un emplacement protégé : un programme légitime qui outrepassé ses droits à cet endroit reçoit des données factices ou se voit refuser l'accès, tandis qu'un programme inconnu ou compromis est rejeté ou suspendu. Le jeton d'actualisation lui-même n'est jamais divulgué.

Revision #1

Created 2026-07-24 06:52:13 UTC by Dennis Underwood

Updated 2026-07-24 06:52:13 UTC by Dennis Underwood