AYI NEDJIMI Consultants

Race Condition : Faille, Attaque et Défense -

9 mai 2026 • Mis à jour le 17 mai 2026 • 28 min de lecture • 5756 mots

Guide exhaustif sur les race conditions : fondamentaux TOCTOU, exploitat
packet attack PortSwigger, CVE Dirty COW et Dirty Pipe, outils Turbo Intru
défensives complètes (verrous ACID, idempotency keys, tests CI/CD). Pou
développeurs et architectes sécurité 2026.

La **race condition**, ou condition de concurrence, est l'une des vulnérabilités les plu
du paysage applicatif moderne. Longtemps cantonnée aux discussions théoriques
concurrente, elle s'est imposée en 2024-2026 comme un vecteur d'attaque critiq
comme la *single-packet attack* introduite par James Kettle de PortSwigger. Cette
temporelle infinitésimale durant laquelle un système traite plusieurs requêtes en p
synchronisation appropriée, permettant aux attaquants de contourner des contrôl
des transactions financières, abuser de codes promotionnels, ou même comprom
d'authentification multifacteur. Comprendre les race conditions exige de maîtriser
théoriques de la concurrence (TOCTOU, atomicité, s et les techn
d'exploitation web modernes (multiplexage HTTP/2, nization, Tu

exhaustif détaille les mécanismes, l'histoire, les outils, les cas d'exploitation réels
indispensables pour tout pentester, développeur ou architecte sécurité opérant en

Qu'est-ce qu'une race condition ?

Une race condition (condition de concurrence) survient lorsque le comportement
l'ordre relatif d'exécution d'opérations concurrentes, sans qu'aucun mécanisme d
un ordre déterministe. Le terme provient de l'analogie d'une "course" entre plusie
requêtes qui tentent d'accéder simultanément à une ressource partagée.

Formellement, une race condition implique trois conditions nécessaires : **concurre**
d'exécution actifs simultanément), **partage de ressource** (une variable, un fichier,
données, un état applicatif accessible aux deux flux), et **absence d'atomicité** (l'op
interrompue ou interleavée avec d'autres opérations). Lorsque ces trois condition
fenêtre d'exploitation existe.

Les races conditions ne sont pas des bugs au sens classique du terme : elles repr
comportements émergents qui n'apparaissent que sous des conditions de charge
peut fonctionner parfaitement pendant des années avant qu'un attaquant ne décle
fenêtre vulnérable. Cette caractéristique en fait des failles particulièrement difficile
unitaires classiques ou les audits de code superficiels.

Sur le web moderne, les race conditions exploitent les **fenêtres de sub-état** : des
lesquels une application a vérifié une condition (solde suffisant, code promo non u
mais n'a pas encore persisté la conséquence de cette vérification. Un attaquant q
plusieurs requêtes simultanément dans cette fenêtre peut déclencher plusieurs fo
si elle n'avait été autorisée qu'une seule fois.

Réponse sous 24h

Devis gratuit →