

O que é um token de atualização (refresh token) e por que perdê-lo é especialmente prejudicial?

Resposta breve: Um token de atualização (refresh token) é uma credencial de longa duração usada para obter silenciosamente novos tokens de acesso sem que o usuário precise fazer login novamente. É nisso que a função "lembrar-me" se baseia. Como ele pode gerar acesso renovado indefinidamente, um token de atualização roubado pode conceder a um invasor acesso duradouro muito depois de sua sessão terminar.

Token de acesso vs. token de atualização

- **Token de acesso (token de sessão):** de curta duração, usado a cada solicitação, expira em minutos ou horas.
- **Token de atualização (refresh token):** de longa duração, usado apenas para solicitar novos tokens de acesso. Às vezes válido por semanas ou meses.

Um token de acesso roubado eventualmente expira. Um token de atualização roubado pode ser usado para gerar novos tokens de acesso repetidamente — o que transforma um roubo único em acesso persistente.

Por que "lembrar-me" é uma troca (trade-off)

Permanecer conectado exige armazenar algo duradouro no dispositivo. Essa conveniência é exatamente o que torna o token armazenado valioso para um invasor. Os armazenamentos de credenciais de navegadores e aplicativos são locais padronizados e previsíveis, portanto ferramentas automatizadas vão diretamente até eles.

Reduzindo o dano

Revogar um token de atualização invalida o acesso que ele pode gerar — é por isso que "sair de todos os dispositivos" e a revogação de tokens são importantes após qualquer suspeita de comprometimento. Mas a revogação é uma resposta *após* o roubo.

A abordagem da Cyber Crucible é impedir a leitura. O armazenamento de credenciais é um local protegido: um programa legítimo que ultrapassa seus limites ali recebe dados falsos ou tem o acesso negado, enquanto um programa desconhecido ou comprometido é rejeitado ou suspenso. O token de atualização em si nunca é entregue.

Revision #1

Created 2026-07-24 05:41:58 UTC by Dennis Underwood

Updated 2026-07-24 05:41:58 UTC by Dennis Underwood