

¿Qué es un token de actualización (refresh token) y por qué su pérdida es especialmente perjudicial?

Respuesta breve: Un token de actualización (refresh token) es una credencial de larga duración que se usa para obtener silenciosamente nuevos tokens de acceso sin que el usuario tenga que iniciar sesión de nuevo. Es en lo que se basa la opción "recordarme". Debido a que puede seguir generando accesos nuevos indefinidamente, un token de actualización robado puede otorgar a un atacante acceso duradero mucho después de que finalice su sesión.

Token de acceso frente a token de actualización

- **Token de acceso (token de sesión):** de corta duración, se utiliza en cada solicitud y expira en minutos u horas.
- **Token de actualización:** de larga duración, se utiliza únicamente para solicitar nuevos tokens de acceso. A veces es válido durante semanas o meses.

Un token de acceso robado eventualmente expira. Un token de actualización robado puede utilizarse para generar nuevos tokens de acceso repetidamente, lo que convierte un robo puntual en un acceso persistente.

Por qué "recordarme" implica una compensación

Permanecer conectado requiere almacenar algo duradero en el dispositivo. Precisamente esa comodidad es lo que hace que el token almacenado resulte valioso para un atacante. Los almacenes de credenciales de navegadores y aplicaciones son ubicaciones estándar y predecibles, por lo que las herramientas automatizadas van directamente a ellos.

Cómo reducir el daño

Revocar un token de actualización invalida el acceso que este puede generar, razón por la cual "cerrar sesión en todos los dispositivos" y la revocación de tokens son importantes tras cualquier sospecha de compromiso. Sin embargo, la revocación es una respuesta *posterior* al robo.

El enfoque de Cyber Crucible consiste en impedir la lectura. El almacén de credenciales es una ubicación protegida: un programa legítimo que intenta acceder de forma indebida recibe datos falsos o se le deniega el acceso, mientras que uno desconocido o comprometido es rechazado o suspendido. El token de actualización en sí nunca se entrega.

Revision #1

Created 2026-07-24 01:43:53 UTC by Dennis Underwood

Updated 2026-07-24 01:43:53 UTC by Dennis Underwood