

Was sind Browser-Cookies, und wie missbrauchen Angreifer sie?

Kurze Antwort: Cookies sind kleine Datenstücke, die eine Website in Ihrem Browser speichert, und einige davon sind Authentifizierungs-Cookies, die Sie eingeloggt halten. Deren Diebstahl ist funktional gleichbedeutend mit dem Diebstahl einer aktiven Sitzung — der Angreifer kann sie in seinen eigenen Browser laden und dabei als Sie erscheinen.

Nicht alle Cookies sind gleich wichtig

- **Präferenz-Cookies** — Sprache, Design, Layout. Geringer Wert.
- **Analyse-Cookies** — Nutzungsmessung. Geringer Wert.
- **Authentifizierungs-/Sitzungs-Cookies** — belegen, dass Sie eingeloggt sind. **Hoher Wert.**

Angreifer interessieren sich fast ausschließlich für die dritte Kategorie.

Warum Cookie-Diebstahl wirksam ist

Ein gestohlenes Authentifizierungs-Cookie löst in der Regel kein Login-Ereignis, keine Passwortabfrage und keine MFA-Aufforderung aus. Die Sitzung existiert bereits; der Angreifer legt lediglich einen Nachweis dafür vor. Aus Sicht der Anwendung sieht dies wie gewöhnliche fortlaufende Aktivität aus.

Browser speichern Cookies auf jedem Betriebssystem an bekannten, vorhersehbaren Speicherorten, sodass automatisierte Tools sie finden können, ohne etwas über den konkreten Rechner zu wissen.

Warum der Browser ein zentraler Angriffspunkt ist

Der Browser bewahrt Cookies, gespeicherte Passwörter, OAuth-Token und den Verlauf an einem Ort auf, was ihn zum reichhaltigsten Identitätsziel auf den meisten Endpunkten macht. Cyber Crucible hat dies direkt beobachtet: Ab dem vierten Quartal 2023 stiegen automatisierte

Reaktionen auf Chrome-, Edge- und Chromium-Aktivitäten von null auf Tausende, mit dazugehörigen CVEs, die später von Google und Microsoft veröffentlicht wurden.

Schutz

Der Browser-Anmeldedatenspeicher ist einer der geschützten Identitätsorte. Ein Prozess, der versucht, darauf zuzugreifen, wird im jeweiligen Kontext bewertet — ein kompromittierter Browser wird ganz anders behandelt als ein unversehrter, und in keinem der beiden Fälle erhält eine übergriffige Anfrage das echte Cookie.

Revision #1

Created 2026-07-24 04:29:15 UTC by Dennis Underwood

Updated 2026-07-24 04:29:15 UTC by Dennis Underwood