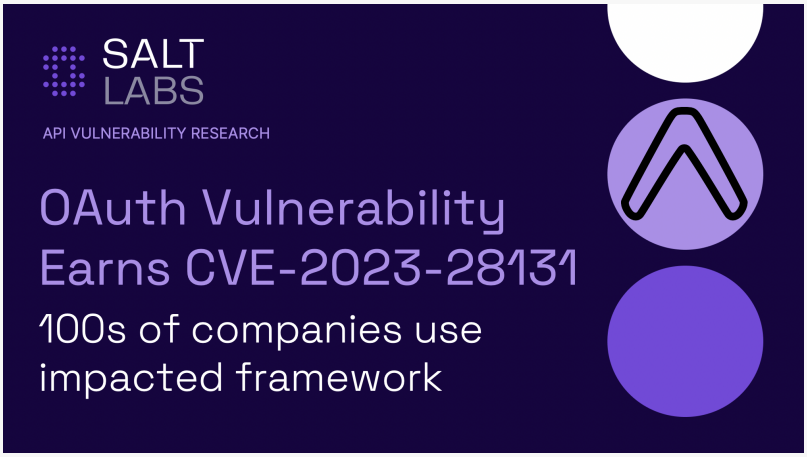
Salt Security Uncovers API Security Flaws in Expo Framework – Issues have been Remediated

Salt Labs researchers identified OAuth vulnerabilities in the popular framework used by more than 100 applications and websites, assigned with CVE-2023-28131



OAuth vulnerability earns CVE-2023-28131

LONDON, UNITED KINGDOM, May 24, 2023 /EINPresswire.com/ -- Salt Security, the leading API security company, today released new threat research from Salt Labs that details several critical security flaws in the Expo framework. The flaws were found in the implementation of the Open Authorization (OAuth) social-login functionality utilised by Expo which had the potential to affect any users logging in to an online service using the Expo framework through their Facebook, Google, Apple, and Twitter accounts. These findings mark the second research report in the Salt Labs OAuth hijacking series, following vulnerabilities uncovered in Booking.com earlier this year.

> With OAuth rapidly becoming the industry standard, bad actors are tirelessly at work to find security vulnerabilities within it."
>
> *Yaniv Balmas, VP of Research, Salt Security*

The Expo research illustrates how enterprises can be subject to API security vulnerabilities introduced by third-party frameworks, in this case potentially affecting the implementation of hundreds of sites and applications. The findings showed that services using this framework were susceptible to credential leakage and could have allowed for large-scale account takeover (ATO) on customers' accounts, enabling bad actors to:

- Manipulate platform users to gain complete control over their accounts
- Leak Personal Identifiable Information (PII) and other sensitive user data stored internally by the sites
- Steal user identities, perform financial fraud, and gain access to credit card information

- Potentially perform actions on behalf of the compromised user within Facebook, Google, Twitter, and other online platforms

Salt Labs, the research arm of Salt Security and a public forum for API security education, discovered the API security gaps and provided the vulnerability analysis. Upon discovering the vulnerabilities, Salt Labs' researchers followed coordinated disclosure practices with Expo. Expo issued Salt Labs CVE-2023-28131 and swiftly remediated all issues. An Expo investigation found no evidence that these flaws had been exploited in the wild.

"Security vulnerabilities can happen on any website – it's the response that matters," said Yaniv Balmas, VP of Research, Salt Security. "With OAuth rapidly becoming the industry standard, bad actors are tirelessly at work to find security vulnerabilities within it. Misimplementation of OAuth can have a significant impact on both companies and customers as they leave precious data exposed and organizations must stay on the pulse of security risks that exist within their platforms."

Vulnerability may impact 100s of companies using Expo, including Codecademy and others
As a framework to develop mobile applications, Expo allows developers to build high-quality native apps for iOS, Android, and web platforms using a single codebase. It provides a set of tools, libraries, and services that simplifies and accelerates the development process.

Salt Labs researchers discovered security vulnerabilities in the social login functionality used by Expo, implemented with an industry-standard protocol called OAuth. Popular across websites and web services, OAuth lets users leverage a "one click" login to access sites using their social media accounts, instead of the more traditional user registration and username/password authentication.

OAuth is popular in large part because it provides users with a much easier experience in interacting with websites. However, its complex technical back end can lead to implementation mistakes that create security gaps with the potential for exploitation. By manipulating certain steps in the OAuth sequence on the Expo site, Salt Labs researchers found they could hijack sessions and achieve account takeover (ATO); steal user data such as credit card numbers, private messages, and health records; and perform actions on behalf of users.

With the potential to impact hundreds of companies using Expo, Salt Labs discovered this vulnerability in Codecademy.com, a popular online platform offering free coding classes across a dozen programming languages. Companies including Google, LinkedIn, Amazon, Spotify, and others use the site to help train employees, and the site boasts ~100 million users. The Salt Labs team was able to exploit the Expo vulnerability on the Codecademy site to gain complete control of accounts.

According to the Salt Security State of API Security Report, Q3 2022, Salt customers experienced a 117% increase in API attack traffic while their overall API traffic grew 168%. The Salt Security API

Protection Platform enables companies to identify risks and vulnerabilities in APIs before they are exploited by attackers, including those listed in the OWASP API Security Top 10. The platform protects APIs across their full lifecycle – build, deploy and runtime phases – utilizing cloud-scale big data combined with AI and ML to baseline millions of users and APIs. By delivering context-based insights across the entire API lifecycle, Salt enables users to detect the reconnaissance activity of bad actors and block them before they can reach their objective. The exploits the Salt Labs team performed would have immediately triggered the Salt platform to highlight the attack.

To learn more about Salt Security or to request a demo, please visit https://content.salt.security/demo.html.

About Salt Security
Salt Security protects the APIs that form the core of every modern application. Its patented API Protection Platform is the only API security solution that combines the power of cloud-scale big data and time-tested ML/AI to detect and prevent API attacks. By correlating activities across millions of APIs and users over time, Salt delivers deep context with real-time analysis and continuous insights for API discovery, attack prevention, and hardening APIs. Deployed quickly and seamlessly integrated within existing systems, the Salt platform gives customers immediate value and protection, so they can innovate with confidence and accelerate their digital transformation initiatives. For more information, visit: https://salt.security/

Bethany Smith
Eskenzi PR
+44 20 7183 2843
email us here