Salt Security Discovers Flaws in Social Login Mechanism Impacting Thousands of Websites

API security vulnerabilities found in OAuth protocol implementations of Grammarly, Vidio, and Bukalapak remediated, but similar issues may impact other sites

LONDON, UNITED KINGDOM, October 24, 2023 /EINPresswire.com/ -- Salt Security, the leading API security company, today released new threat research from Salt Labs highlighting API security vulnerabilities uncovered in the social sign-in and Open Authentication (OAuth) implementations of multiple online companies, including Grammarly, Vidio, and Bukalapak. The flaws, which have since been remediated, could have allowed for credential leakage and enabled full account takeover (ATO). Salt Labs also reported that 1000s of other websites using social sign-in mechanisms are likely vulnerable to the same type of attack, putting billions of individuals around the globe at risk.

These findings mark the third and final research report in the Salt Labs OAuth hijacking series, following vulnerabilities uncovered in Booking.com and Expo earlier this year.

This latest research identified flaws in the access token verification step of the social sign-in process, part of the OAuth implementation on these websites. The vulnerabilities could have impacted nearly a billion user accounts across these three sites.

The vulnerabilities identified could allow cyber criminals to:

- Gain complete access to a user's accounts on dozens of websites, potentially allowing access to bank accounts, credit card details, and other sensitive data

- Perform any action on behalf of that user which may lead to identity theft and financial fraud

Favoured across many websites and web services, OAuth enables a "one-click" login that lets users tap their social media accounts, such as Google or Facebook, to verify their identity and

register on a site rather than set up a unique username/password combination for access. For this type of login, OAuth needs a verified token to approve access, and all three sites failed to verify the token. As a result, the Salt Labs researchers were able to insert a token from another site as a verified token and gain access to user accounts - using a technique called “Pass-The-Token Attack.”

Vidio

Vidio, an online video streaming platform with 100M monthly active users, offers a range of content, including movies, TV shows, live sports, and original productions.

Salt Labs’ researchers discovered OAuth security vulnerabilities when logging in through Facebook. Because the Vidio.com site did not verify the token, which the website developers must do, and not OAuth itself, an attacker could manipulate the API calls to insert an access token generated for a different application. This alternate token/AppID combination allowed the Salt Labs research team to impersonate a user on the Vidio site, which would have allowed massive account takeover on thousands of accounts.

Bukalapak

Bukalapak is one of Indonesia's largest and most prominent eCommerce platforms, with more than 150 million monthly users.

Like Vidio, Bukalapak didn’t verify the access token when users registered using a social login. Therefore, by inserting a token from another website, the Salt Labs team could access a user's credentials in bukalapak.com and completely take over that user’s account.

Grammarly

Grammarly.com is an AI-powered writing tool that helps users improve their writing by offering grammar, punctuation, spelling checks, and other writing tips to more than 30 million daily users.

By doing reconnaissance on the API calls and learning the terminology the Grammarly site uses to send the code, the Salt Labs team was able to manipulate the API exchange to insert code used to verify users on a different site and, again, obtain the credentials of a user’s account and achieve full account takeover.

Upon discovering the vulnerabilities on all three sites, Salt Labs’ researchers followed coordinated disclosure practices, and all issues have been remediated.

“OAuth is one of the fastest adopted technologies in the AppSec domain and has quickly become one of the most popular protocols for both user authorisation and authentication,” said Yaniv

Balmas, VP of Research, Salt Security. “The Salt Labs research illustrates the potential impacts that OAuth implementation issues can have on a business and its customers. We hope this series has helped educate the broader industry on the nature of potential OAuth implementation errors and how to close these API-based security gaps to better protect data and use OAuth more securely.”

The Salt Security State of API Security Report, Q1 2023, showed a 400% increase in unique attackers in the last six months, with 43% of respondents stating account takeover (ATO) as a high concern. The Salt Security 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 into API threats and vulnerabilities, including those outlined in the OWASP API Security Top 10 list.

The full report, including how Salt Labs conducted this research and steps for mitigation, is available here. To learn more about Salt Security and its platform, or to request a demo, please visit https://content.salt.security/demo.html.

If you will be onsite at SecTor, Aviad Carmel and Yaniv Balmas will be hosting a speaking session titled: Uh-OAuth! - Breaking (and Fixing) OAuth Implementations” - Wednesday, October 25, 4:00-5:00pm, Meeting Room 718A.

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/

Charley Nash
Eskenzi PR
charley@eskenzipr.com

---

in today's world. Please see our Editorial Guidelines for more information.