Salt Security Addresses Critical OAuth Vulnerabilities By Enhancing API Security Platform with OAuth Protection Package

Salt's multi-layered protection package was created to detect attempts aiming to exploit OAuth and proactively fix vulnerabilities

LONDON, UNITED KINGDOM, April 25, 2024 /EINPresswire.com/ -- Salt Security, the leading API security company, today announced the release of its new multi-layered OAuth protection package to detect attempts to exploit OAuth and proactively fix vulnerabilities. Salt is enhancing its API protection platform with a comprehensive suite of new OAuth threat detections and posture rules to address the growing challenge of OAuth exploitation. The company is the first API security vendor to launch deep OAuth threat detection capabilities, and these innovations will empower organisations to identify and mitigate malicious attempts to exploit OAuth flows, ultimately safeguarding sensitive data and user accounts.

> Organisations that demonstrate a commitment to robust security practices foster user confidence and enhance brand reputation, leading to stronger customer relationships and a competitive edge."
>
> *Yaniv Balmas, Vice President of Research, Salt Security*

Today, OAuth is an important part of modern authorisation frameworks, granting access to resources across different applications easily. However, vulnerabilities in OAuth implementations can create significant security risks. By implementing strong OAuth security controls, organisations can safeguard their users' data, prevent unauthorised access to critical resources, and maintain user trust.

Salt Security's recent investigation exposed several critical security flaws within the OAuth implementations of popular ChatGPT plug-ins. ChatGPT plugins enable ChatGPT to interact with the outside world and third-party websites like Google Drive, GitHub, Emails, and more. Beyond this most recent example of OAuth threats with ChatGPT, the

Salt Labs team found several other OAuth-specific exploitable vulnerabilities within Booking.com, Grammarly, Vidio.com, and Expo/CodeCademy, indicating the critical need for tools to help find and mitigate these types of risks before attackers can take advantage. These real-world examples underscore the importance of robust security measures to thwart sophisticated OAuth attack tactics before they can inflict significant damage.

With these new capabilities, the Salt platform will address:

- Access Token and Authorisation Code Theft: Vulnerabilities in OAuth systems can leave access tokens or authorisation codes susceptible to theft. Attackers can leverage those stolen elements to impersonate legitimate users and gain unauthorised access to sensitive resources and applications.
- Increasing OAuth Attacks: OAuth has been in widespread use for over a decade but we have seen attacks on the rise. This is caused by organisations' increased usage of APIs and microservices making OAuth even more popular while increasing the complexity of securing it. Attackers have taken advantage of this by crafting specific OAuth-based attacks with continuing attempts to find additional OAuth vulnerabilities to exploit.

Salt Security's OAuth Protection Package provides robust OAuth defences that help organisations achieve several critical security objectives. With these enhancements, customer accounts, intellectual property and authorisation tokens will be shielded from malicious actors who are tirelessly at work attempting to exploit vulnerabilities in OAuth implementations. In fact, within just five days of the OAuth protection package being deployed for Salt customers, it detected an OAuth vulnerability within a large financial institution. With the information on the detection, the customer was able to rapidly fix the vulnerability, preventing it from being exploited by threat actors.

"Organisations that demonstrate a commitment to robust security practices foster user confidence and enhance brand reputation, leading to stronger customer relationships and a competitive edge in the marketplace," said Yaniv Balmas, Vice President of Research, Salt Security. "With the rise in OAuth specific vulnerabilities, it is vital for organisations to incorporate robust security measures to thwart sophisticated OAuth attack tactics before they can inflict significant damage. By implementing strong OAuth security controls, organisations can safeguard their users' data, prevent unauthorised access to critical resources, and maintain user trust."

Salt Security's unwavering commitment to research and development ensures that its solutions remain effective against emerging OAuth attack techniques. Salt's proactive approach keeps businesses a step ahead of evolving threats, allowing them to operate with greater confidence and agility.

More details about Salt's new OAuth threat detection capabilities can be found in this blog. To request a demo, please visit https://content.salt.security/demo.html.

About Salt Security

As the pioneer of the API security market, Salt Security protects the APIs that form the core of every modern application. Protecting some of the largest enterprises in the world, Salt's 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. With its patented approach to blocking today's low-and-slow API attacks, only Salt provides the adaptive intelligence needed to protect APIs. Salt's posture governance engine also delivers operationalised API governance and threat detection across organisations at scale. Unlike other API governance solutions, Salt Security's AI-based runtime engine pulls from the largest data lake in order to continuously train the engine. Salt supports organisations through the entire API journey from discovery to posture governance and threat protection. 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
