EINPRESSWIRE

Oxeye Identifies Exploit Exposing PII in Online Payment Services

Exploit Leverages Jaegar to Access Sensitive User Data

Oxeye Logo

TEL AVIV, TEXAS, ISRAEL, December 20, 2021 /EINPresswire.com/ -- Oxeye research operations has identified an exploit while trying to create an access path using Jaegar, an open-source software for tracing transactions between distributed services. During its examination, Oxeye discovered Jaegar lacked a login and password which allowed access to user data collected/stored by open-source service instrumentation platform OpenTelemetry. As a result, unauthorized purchases on user accounts were made possible.

The research performed by Oxeye revealed that the Jaeger UI was publicly exposed and did not require credentials for access. In the Jaeger dashboard, both internal and external microservices were visible, as were the connections between microservices. Because many approaches to tracing are implemented in a way where the APIs' actual parameters are sent via POST parameters, they are not shown in Jaeger. But, when the parameters were sent through the GET parameter they were visible – resulting in the aforementioned security issue.

Oxeye discovered the exploit with one online payment service. The problem was reported to the provider, citing a backdoor path via unprotected exposure to the Internet. This could allow web page refresh tokens of recently reviewed pages held in Jaegar to open access to user PII. When made aware of the exploit, the online payment provider immediately closed the Internet access to the identified Jaegar which resolved the problem.

Additionally, a second identified endpoint that contained sensitive information. Its purpose included verification of the refresh token for authenticated users. During the process, the refresh token would be sent to an internal gateway using the GET parameter. After finding refresh tokens from other accounts, the ability to generate an access token and bypass the authentication mechanism was discovered. Then after looking into the cookies, the system could be orchestrated to request a new access token and backdoor entry to the platform. This issue has also been addressed.

“While initially looking to show the communication between microservices in these environments, it was realized that the payment provider’s platform was exposed via sensitive data presented in the open Jaeger. Through this security gap, it was possible to login and authenticate into the platform as another user (which was accomplished several times),” commented Ron Vider, CTO and Co-Founder of Oxeye. “This means that a hacker with malicious intent could easily take advantage of this misconfiguration issue and steal the sensitive and PII data of clients. Credit card information as well as sensitive technical data could be used maliciously by using connections between microservices, APIs, etc.”

According to the Federal Bureau of Investigation (FBI), victims of online or internet-enabled crime are advised to file a report with the Internet Crime Complaint Center (IC3) as soon as possible. Crime reports are used for investigative and intelligence purposes. Rapid reporting can also help support the recovery of lost funds. Visit ic3.gov for more information, including tips and information about current crime trends.

Since reporting the exploit, the payment provider has removed the Jaeger dashboard from exposure to the Internet, resolving the potential for unauthorized access. Oxeye, a specialist in cloud-native Application Security Testing will make every effort to notify application providers of exploits when discovered by the company’s technology platform and team of researchers.

About Oxeye
Oxeye provides a cloud-native application security testing solution designed specifically for modern architectures. The company enables customers to identify and resolve the most critical code vulnerabilities as an integral part of the software development lifecycle, disrupting traditional application security testing (AST) approaches by offering a contextual, effortless, and comprehensive solution that ensures no vulnerable code ever reaches production. Built for Dev and AppSec teams Oxeye helps to shift-left security while accelerating development cycles, reducing friction, and eliminating risks.

Joe Austin
Public Relations
+ 18183326166
email us here
Visit us on social media:
Twitter
LinkedIn

---

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