Examining Security Risks in Logistics APIs Used by Online Shopping Platforms

We examined the security flaws that we found in the logistics API implementation of e-commerce platforms that can potentially leak the personally identifiable information (PII) of consumers. We also discuss the security risks and implications that such flaws present for software engineers, e-commerce platform providers and consumers, and provide recommendations on how the flaws can be addressed.

Key Findings

- PII can be leaked in many ways. One way is through the transmission of URL query parameters between e-commerce platforms and logistics APIs. We found that it is possible for unauthorized parties to retrieve customers' PII by directly accessing URLs that do not require users to authenticate the session.
- The use of unencrypted URL query parameters renders the PII susceptible to sniffing and man-in-the-middle attacks.
- The use of session and cookies that have no set expiration by some third-party logistics (3PL) providers also poses a risk for PII leakage, which is noncompliance to the Open Web Application Security Project's (OWASP) recommendation of setting specific expiration dates to regulate authentication.

Security Recommendations

- Software developers for e-commerce API should determine what data needs to be provided throughout the course of the transaction and what authentication measures should be used to prevent data from being exposed to accounts with access restrictions or limited privileges.
- Transactions that involve the exchange of PII to a third party should be done properly by encrypting data and authenticating requests each time PII is transmitted.
- Consumers should avoid the installation of unknown browser extensions to web browsers that can read and collect unencrypted URL query strings.

The large-scale use of e-commerce platforms has made logistics APIs a necessity, so it is critical to secure them. Neglecting to do so exposes users to data leaks that enable malicious actors to devise more attacks that can cause more harm. Therefore, establishing a proactive cybersecurity approach early on is key to make online shopping platforms a safe space for consumer

Trend Micro Solutions

Trend Micro Cloud One™ – Application Security offers protection and detection capabilities against the latest threats for modern applications and APIs built on your container, serverless, and other computing platforms. Application Security extends your cloud-native application protection strategy to runtime and keeps your developers developing, not spending time on tedious maintenance.

Read our full paper at
https://research.trendmicro.com/EcommerceAPISecurity.

TREND MICRO™ | research