NEWS RELEASE

New Wallarm report exposes API security risks for companies including Netflix and WordPress

11/7/2023

The findings reveal critical and 239 new API vulnerabilities in Q3 that are linked to authentication, authorization and access control

SAN FRANCISCO--(BUSINESS WIRE)-- **Wallarm**, the leading end-to-end API and app security company, today announced the release of its **Q3-2023 Wallarm API ThreatStats™** report. The quarterly report details the surge in threats centered around APIs and uncovers critical vulnerabilities, like injections and API data leaks, that have recently impacted leading firms, including Netflix, VMware and SAP. Wallarm executives will present top findings from the report during a **webinar** on Nov. 8 at 11 a.m. PT/2 p.m. ET.

The new report introduces a revamped “Top 10 API Security Threats” compilation, a real-time data-driven list covering the 239 vulnerabilities discovered during the quarter. Injections, which involve malicious data or code being inserted into an API that leads to unauthorized access and data breaches, ranked first on the list, attacking vectors like SQL and XML. Also making the list were cross-site attacks, broken access control and poor session and password management.

Of the 239 vulnerabilities, 33% (79 out of 239) were associated with authentication, authorization and access control (AAA) — foundational pillars of API security. Open authentication (OAuth), single-sign on (SSO) and JSON Web Token (JWT), safeguards for API security, were compromised in reputable tech organizations such as Sentry and WordPress. Sentry experienced incorrect credential validation on OAuth token requests, potentially exposing developers’ projects to unauthorized access, while WordPress’ SSO was subject to plugin broken authentication, leaving its millions of users' data vulnerable to theft.

The growing issue of API data leaks, as company tech stacks get more complicated, was also a focal point of this quarter's report. Although relatively new, API data leaks ranked fourth on the security threats list due to their potential for unrestrained disclosure of sensitive data, often through negligent methods. Evidence of these risks is found in the recent serious data breaches suffered by Netflix, VMware and SAP, with Netflix exposing JWT secret keys in error messages and VMware disclosing sensitive information vulnerabilities.

"We saw in recent months that even major players like Netflix and VMware aren't exempt from significant data exposures," said Ivan Novikov, CEO of Wallarm. "Whether caused by malicious actors or internal carelessness, this report is a wake-up call for business leaders and cybersecurity professionals to include protection against threats to APIs and other leaks in their product security programs. Established security frameworks, like OWASP API Security Top-10, are one way to get started but have limitations in addressing today's complex API security needs. This real-time data-driven threat list complements and extends the OWASP framework by identifying unaddressed threats and vulnerabilities, enhancing overall security posture."

Combating the API security threats highlighted starts with a proactive security strategy. The report provides key expert insights and recommendations for navigating this complex cyber landscape, including prioritizing AAA principles with regular updates to mitigate potential risks and incorporating API leak protection measures like an automatic discovery system to block threat actors from using leaked API keys.

To view the full Q3-2023 Wallarm API ThreatStats™ report, please visit **here**.

To learn further insights from the report, please **register for the webinar**.

About Wallarm

Wallarm, the integrated App and API Security company, provides robust protection for APIs, web applications, microservices, and serverless workloads running in cloud-native environments. Wallarm is the preferred choice of hundreds of Security and DevOps teams for comprehensive discovery of web apps and API endpoints, protection against emerging threats throughout their API portfolio, and automated incident response to enhance risk management. Our platform supports modern tech stacks, offering dozens of deployment options in cloud and Kubernetes-based environments, and also provides a full cloud solution. Wallarm is headquartered in San Francisco, California, and is backed by Toba Capital, Y Combinator, Partech, and other investors.

Sara Black
PRforWallarm@bospar.com

Girish Bhat

girish@wallarm.com

Source: Wallarm