Wallarm Q2 Report Reveals Sharp Rise in API Vulnerabilities & Exploits

Compared to Q1, API vulnerabilities rose +268%; impacted more vendors +270% and grew in criticality rating +90%

wallarm
WEBINAR
Q2 API Vulnerability Report:
Are APIs Really A Threat?
Monday, August 8th, 11:00 AM PDT

San Francisco, California Jul 28, 2022 (Issuewire.com) - APIs are at greater risk today than they were even one quarter ago, according to a new report from Wallarm, a leading API Security vendor. As will be discussed in the upcoming webinar on August 8th, the *Q2 2022 API Vulnerability and Exploit Report* found that API vulnerabilities were more prevalent (+268%), farther-reaching (+270%), and increasingly critical (90%), which further escalates the risk to today's API portfolios and the need for API security.

In Q2, Wallarm collected and analyzed 184 API vulnerabilities (an average of 2 per day) compared to just 50 last quarter. Overall, these vulnerabilities impact 111 different vendors (up from 30 in Q1) and 53 percent of them are rated critical or high compared to 28 percent which received that rating in Q1. More than one-third of the vulnerabilities are almost immediately exploited.

Gartner predicts that in 2022, API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications. Midway through the year, this forecast is proving true.

“As the API market continues its high growth trajectory, so too does the risk associated with them,” says Ivan Novikov, CEO, and co-founder of Wallarm. “Expanding vulnerability management efforts to include APIs requires visibility across the entire API portfolio, assessment and triage of vulnerabilities as they arise, and ensuring mitigations are implemented both in code and at run-time.”

Some of the highlights which will be in the final Q2 API vulnerability report include:

- API threats grew 3.7x QoQ and already hit the 2 new exploits a day threshold.
- Critical and High-risk API vulnerabilities have increased dramatically, to 53% of the total.
- Injections (OWASP A03 / API8) are now the highest risk for APIs, ahead of BOLA by all metrics (number of discovered issues, exploitability and severity).
- 33% of the reported API vulnerabilities are almost immediately exploited, with PoCs published within a median of 2-½ weeks.

Wallarm continually collects and analyzes published API vulnerabilities and exploits. Researchers dissect the data to look for trends and insights from a variety of perspectives, including software type, vendor, CVSS scores, CWEs, and both OWASP Top-10 (2021) for web apps and OWASP API Security Top-10 (2019). Publicly disclosed exploit POCs are also reviewed to understand if and when the threat has moved from theoretical to actual.

Learn more about the Q2-2022 API Vulnerability Report and download the infographic in this blog post.

Q2 API Vulnerability Report Webinar

Register to attend our upcoming webinar for a deep dive into the data and the implications:

Date: Monday, Aug 8, 2022

Time: 11:00am PT / 2:00pm ET

Title: **Q2 API Vulnerability Report: Are APIs Really A Threat?**

Speaker: Ivan Novikov, CEO & co-founder of Wallarm

Registration: http://lab.wallarm.com/2022-q2-vulnerability-report-webinar/

About Wallarm

Wallarm end-to-end API security products provide robust protection for APIs, microservices, and serverless workloads running in cloud-native environments. Hundreds of Security and DevOps teams chose Wallarm to get unique visibility into malicious traffic, robust protection across the whole API portfolio, and automated incident response for product security programs. The company is committed to supporting 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.

Media Contact

Wallarm

media@wallarm.com

+1 (415) 940-7077

Source : Wallarm

See on IssueWire