wallarm

EXECUTIVE SUMMARY

2024 API ThreatStats™

Findings, Insights and Predictions

>1.2 Billion
attacks detected last year

>22,000
CVEs examined

146
Bug Bounty reports analyzed

This report provides a comprehensive overview of API security threats and is a vital resource for Security, Engineering and DevOps professionals. We've prepared a Top-10 list of risks based on an extensive analysis of real attacks detected by Wallarm, and examining all API-related CVEs and Bug Bounty reports from the last year. This is a must-read to understand the developments of 2023 and how to prepare for evolving API threats in 2024.

Key API Security Findings

The analysis of recent data has yielded several intriguing insights into the trends in API security. There is a rising trend in API Security threats with a noticeable increase in both the number and severity of attacks and vulnerabilities related to APIs. Specifically, we observed:

1 Increase in the Volume of API Vulnerabilities

30% increase in API-related Common Vulnerabilities and Exposures (CVEs) and security bulletins in 2023 compared to 2022, amounting to 846 issues for the year.

2 Growth in Malicious API Requests

The proportion of malicious requests involving APIs that were blocked by Wallarm rose significantly by 16%, **from 54% in 2022 to 70% in 2023**, among all application attacks.

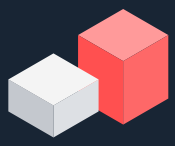
3 Significant Presence in CISA KEV Vulnerabilities

API-Related Vulnerabilities Doubling: A significant portion of CISA KEV vulnerabilities are API-related. 20% of all the vulnerabilities listed in the CISA Known Exploited Vulnerabilities (KEV) are now API-related, a marked increase from just 10% in 2017, doubling over five years.

4 Dominance of API Security in the Bug Bounty Landscape

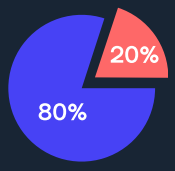
In 2023, majority of bounties were for API security: **62% of all bounty payments, totaling $158,000**, were awarded for identifying API bugs, up from 59% in 2022.

30%
increase in **API related vulnerabilities**



16%
increase of **malicious requests involving APIs** blocked by Wallarm

20%
of all the vulnerabilities listed in the **CISA KEV are now API-related**



62%
of bug bounty rewards are for **API bug discoveries**

Top-10 API Security Risks for 2024

Real-time, data-driven APIs risk taxonomy

Security teams require a framework to prioritize their efforts in API security programs. To create a guide for 2024, we conducted an in-depth analysis of the actual vulnerabilities and attacks that occurred last year, affecting customers in industries such as technology, media, retail, financial services, and others. Here are the Top-10 threats to tackle.

Rank #	Risk Type	Class Description
1	**Injections**	Attack vectors like SQL, XML, and Command Injections.
2	**Authentication Flaws**	Issues where identity verification fails.
3	**Cross-site Issues**	Includes CSRF, XSS and other threats targeted across different sites.
4	**API Leaks**	Leaking sensitive information such as API Keys, JWT tokens, etc.
5	**Broken Access Control**	Access governance loopholes that may lead to unauthorized data exposure.
6	**Authorization Issues**	Lapses in resource access controls post-authentication.
7	**Insecure Resource Consumptions**	Server exhaustion and service disruptions.
8	**Weak Secrets and Cryptography**	Issues like hard-coded secrets or weak encryption algorithms.
9	**Sessions and Password Management**	Inadequate session handling and poor password management schemes.
10	**Server-Side Request Forgery (SSRF)**	Server-Side Request Forgery attacks, distinct from injections.

Not covered in OWASP: API Leaks. Threat #4

As a benchmark, many have turned to OWASP API Security Top 10 to identify API-related threats. Despite not being covered in the OWASP API Security guidelines, **API leaks have emerged as a significant threat, yet they are often overlooked.** Data for last year highlights multitude of incidents traced back to leaked credentials (including by 3rd parties) leading to security breaches.

Most Notable API Exploits of the Year

- **Highest H1 Payout for Snapchat:** The most significant bug bounty payout in 2023.
- **Citrix Bleed (CVE-2023-4966):** Memory leak issue in Citrix Netscaler ADC, known for its comprehensive API security functionalities.
- **Johnson OpenBlue Security Bug:** Highlighted by CISA, this is the most well-known hardware API security bug of the year.

CITRIX®

Johnson Controls

2024 API Risks Predictions

Shift Toward API as a Primary Attack Vector

As **more breaches start with an API attack**, the focus on API security as a fundamental aspect of cybersecurity strategies will likely intensify in 2024.

Continued Growth in API Vulnerabilities

A 30% growth in API vulnerabilities from 2022 to 2023 indicates a trend that might continue into 2024. Organizations should be prepared for a larger number of API vulnerabilities and a corresponding increase in the attack surface.

Emergence of API Leaks as a Top Threat

API Leaks are emerging as a **major new risk area**, ranking as the #4 top security threat in the Top 10 API Security Risks for 2023. This trend suggests that in 2024, there will be an increased focus on preventing leaks of sensitive information such as API keys and JWT tokens.

Persistent Exploitation of Log4j

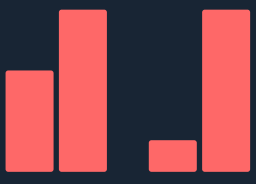
The Log4j vulnerability was **the most exploited in 2023**, indicating that vulnerabilities in pervasive libraries like Log4j might continue to be a major concern in 2024.

Growth of Open-Source Software (OSS) Vulnerabilities

OSS products continue to dominate API vulnerabilities, with a significant jump from **67% in Q4-2022 to 78% in Q1-2023**. This trend may persist into 2024, requiring more attention to the security of OSS products.

Increased Focus on Broken Access Control and Authorization

The shift in focus from Injection to Broken Access Control and Broken Object Level Authorization indicates these areas may become more prominent in API security strategies in 2024.



Rising Number and Sophistication in API Attacks

A marked increase in the number and sophistication of API attacks is evident, with a **60% quarter-over-quarter and 514% year-over-year rise** in unique API attacks. This suggests that 2024 might witness even more sophisticated API attacks, necessitating advanced defense mechanisms.

Adoption of New Metrics for Vulnerability Triaging

The use of alternative metrics like "Google popularity" for triaging vulnerabilities suggests that 2024 might see the adoption of new approaches to assess and prioritize API vulnerabilities.

www.wallarm.com

(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107