wallarm

ANNUAL REPORT

2024 Annual API ThreatStats™ Report

This report provides a comprehensive overview of API security threats and is a vital resource for Security, Engineering and DevOps professionals, offering detailed data, analysis and predictions on API security. It is based on extensive analysis of real data from Wallarm on API and application attacks, totaling over 1.2 billion malicious requests, examining CVEs and Bug Bounty reports in 2023.

Table of contents

Foreword

At Wallarm, our commitment to elevating API security awareness remains a cornerstone of our mission, and we are proud to release the Annual ThreatStats™ Report for 2024. This marks our second year of contributing vital insights to the cybersecurity community through our quarterly and annual API ThreatStats™ publications. Our objective is to continuously monitor and evaluate the dynamic trends in API threats, offering a comprehensive view into the latest attack vectors and vulnerabilities at the forefront of the API economy. API security has risen to prominence as a critical threat confronting businesses in the current landscape. Our report is diligently designed to both quantify and thoroughly analyze this urgent matter.

The 2024 edition of the API ThreatStats™ report, expands its scope beyond CVE data and CVSS-driven risk assessments. It now includes invaluable insights drawn from bug bounty programs and introduces an AI-driven categorization of the Top-10 API Security vulnerabilities and exploits for 2023.

The past year has witnessed an escalating trend in API vulnerabilities.Our report reveals a significant rise in both the frequency and severity of these threats. This trend underscores the evolving sophistication and persistence of cyber adversaries. These adversaries relentlessly pursue new vulnerabilities within our rapidly expanding digital landscape.

Our analysis reveals a notable surge in API-related security incidents, emphasizing the need for robust and innovative defenses. The rise in API vulnerabilities, particularly in internal and private APIs, calls for an immediate reassessment of organizational security strategies. The prevalence of injection vulnerabilities, the sophistication of attacks, and the growing dependence on APIs all contribute to an intensified risk landscape.

A pivotal finding over the course of the previous year has been the increase in API-centric attacks, demonstrating the adversaries' shift in focus towards more sophisticated and targeted exploits. This shift demands a proactive and informed approach to API security, emphasizing the need for comprehensive and adaptable defense strategies.

At Wallarm, we are committed to equip organizations with the means to stay ahead of these evolving threats. Our report offers not just a thorough analysis of the current state of API threats but also provides practical guidance and recommendations to fortify API security. We firmly believe that understanding these threats is the initial step in establishing resilient and effective defense systems.

The foundation of this Annual ThreatStats™Report lies in a comprehensive analysis of a vast compilation of data, examining over 22,000 CVEs from various security bulletins and reports, coupled with a detailed review of 146 Bug Bounty reports. This analysis is augmented by data from Wallarm on API and application attacks, collectively surpassing 1.2 billion incidents. A notable revelation in our report is the 30.15% increase in API-related CVEs and security bulletins in 2023, a significant escalation from the previous year, with 846 issues identified within the year.

As the technology landscape continuously evolves, so does the sophistication of cyber threats. It is crucial that our security strategies evolve correspondingly to protect our digital assets. Wallarm's mission is to deliver the necessary tools, intelligence, and expertise to ensure your organization navigates these challenges with confidence and security.

We trust that this report will be a valuable resource for a diverse audience, including CISOs and security professionals. Our research sheds light on significant trends in the field, from the predominant role of API exploits in bug bounty programs to the distinct differences between the types of exploits observed in 2023 compared to those listed in the 2021 OWASP API Security Top 10.

Ivan Novikov | CEO, Wallarm

Introduction

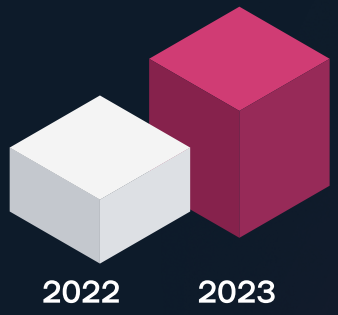
Welcome to the **Wallarm Annual ThreatStats™ Report 2024**. This report offers a comprehensive overview of the API threat landscape throughout the previous year, 2023, along with forecasts and predictions for 2024. This comprehensive report is a compilation of critical insights from regular and quarterly analyses, offering a comprehensive perspective on evolving API security threats. Our team has meticulously compiled and analyzed data to offer valuable insights for cybersecurity professionals.

The report highlights an escalating number of threats specifically targeting APIs, signaling a need for immediate and focused attention from business and cybersecurity leaders. It delves into the constantly evolving nature of these threats, identifying key vulnerabilities and providing in-depth insights and recommendations for navigating this complex landscape.

Key Findings & Insights

Recent data analysis reveals important trends in API security. There's a noticeable increase in threats, characterized by a rise in both the frequency and severity of attacks and vulnerabilities related to APIs. Key observations include:

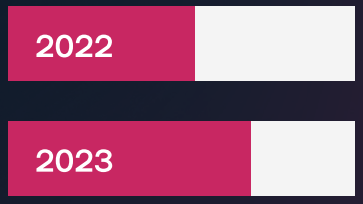
+30%
API related vulnerabilities



Increase in the Volume of API Vulnerabilities

Between 2022 and 2023, there was a rise in API vulnerabilities, escalating from 650 to 846. Additionally, during the same period, there was a modest increase in CVEs, going from 24,454 to 24,559.

+16%
malicious requests involving APIs blocked by Wallarm



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.

62%
of all bounty payments, totaling $158,000, were awarded for API bugs

API Security's Prominence in Bug Bounties

62% of all bounty payments, totaling $158,000, were awarded for identifying API bugs, up from 59% in 2022.

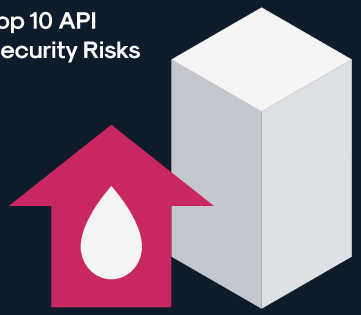
50%
of the Google's Top 20 CVEs are API related

High visibility of API vulnerabilities in Google searches

Half of the top 20 most mentioned vulnerabilities in Google searches are API related, indicating a growing public awareness and concern about API security.

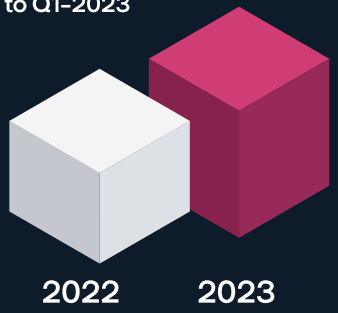
#4

API Leaks in the Top 10 API Security Risks



+ 11%

OSS vulnerabilities from Q4-2022 to Q1-2023



> 52 million

exploitation attempts experienced CVE-2021-44228

Significant Threats from API Leaks

OWASP API Security Top-10 frameworks are vital but don't completely cover modern API leak challenges in organizations. Some examples of Key API leaks in 2023:

- **CVE-2023-49103:** Exposure of configuration details in ownCloud's owncloud/graphapi;
- **CVE-2023-44483:** Private key exposure in Apache Santuario log files;
- **CVE-2023-1387:** Leakage of JWT Tokens in Grafana;
- **CVE-2023-46671:** Disclosure of credentials in Kibana log files.

Growth of Open Source Software (OSS) Vulnerabilities

Open Source Software (OSS) products continue to dominate API vulnerabilities, with the share of open-source in API vulnerabilities increasing from 64.9% in 2022 to 73.6% in 2023. 78% of API vulnerabilities related to OSS with a significant jump from 67% in 2022 to 2023.

Log4Shell / Apache Log4j (CVE-2021-44228)

The significant vulnerability in the popular Apache Log4j 2 Java logging library constituted 33% of all CVEs detected, leading to more than 52 million attempts at exploitation. This emphasizes the continuous risk from threats like Log4Shell, underlining the need for proactive threat detection.

Top 10 API Security Risks

The report underscores the evolving landscape of API security, emphasizing significant changes in the nature of attacks, with a diversification of attack vectors and a notable increase in their sophistication. This evolution signals a pressing need for more advanced security measures. A key element of the report is the revised 'Top 10 API Security Threats' list, which is informed by real-time data and outlines the most critical vulnerabilities identified throughout the year. This compilation is distinct from traditional models like OWASP, as Wallarm employs a tailored methodology and classification focused on critical vulnerabilities unique to the modern API ecosystem.

Limitations of Existing Security Frameworks

What distinguishes Wallarm's methodology from traditional frameworks like OWASP is our unique approach and classification that specifically targets pressing vulnerabilities which are critical in today's modern API ecosystem. Recognizing these threats and their implications enables organizations to take immediate and proactive steps to strengthen their defenses and safeguard critical assets

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.

Top 10 API Security Risks for 2023

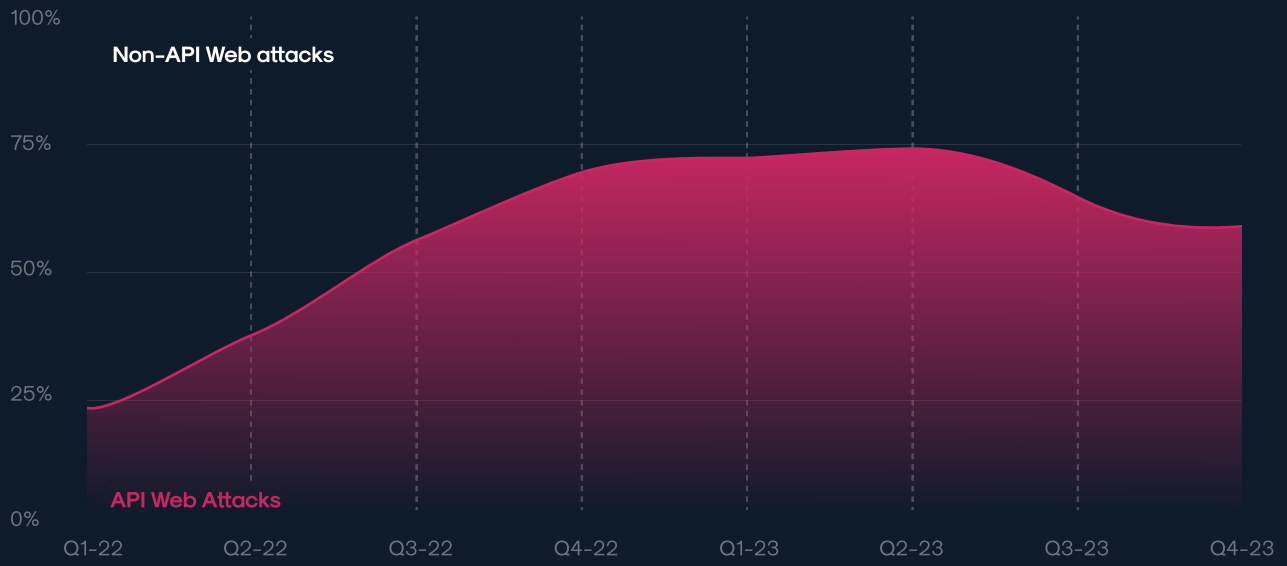
API ThreatStats™ Top 10: Q1-Q4'2023

Don't underestimate traditional vulnerabilities. Traditional app level vulnerabilities are still a major threat.
Based on the ThreatStats™ report, Injections are still the #1 issue, based on the sheer number of vulnerabilities.

Increase in malicious requests related to API

The share of malicious requests blocked by Wallarm related to APIs **increased by 16% (from 54% to 70%)** from 2022 to 2023 among all the application attacks.

When Wallarm WAAP detects an attack, it attempts to attribute the attacks to exploitation of known CVEs. Totally, Wallarm detected exploitation attempts of 860 different CVE vulnerabilities in 2023. Only 11% of them are contained in the CISA KEV catalog.



The change of API attacks share

Top exploited CVE Vulnerabilities observed

When Wallarm identifies an attack, it seeks to link the attack to known CVEs (Common Vulnerabilities and Exposures). The table below shows the top 10 CVE-assigned vulnerabilities that were most exploited in 2023. Notably, none of these top 10 vulnerabilities appear in the CISA Known Exploited Vulnerabilities Catalog (CISA KEV). The most frequently exploited vulnerability was Log4j (CVE-2021-44228), accounting for 33% of all detected incidents.

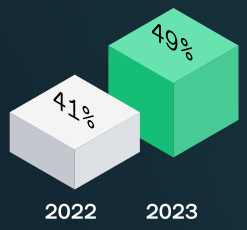
#	CVE	Name	Exploitation attempts	Share of all detected CVE
1	CVE-2021-44228	Remote Code Execution in Apache Log4j (Log4shell)	52,457,688	33%
2	CVE-2021-28169	Arbitrary file read in Eclipse Jetty	8,430,675	5%
3	CVE-2022-42889	Remote Code Execution in Apache Commons Text (Log4Text)	5,084,334	3%
4	CVE-2021-45105	Denial of Service in Apache Log4j2	4,360,371	3%
5	CVE-2013-4810	Code injection in HP Procurve Manager	4,000,474	2%
6	CVE-2017-9841	PHP code injection in PHPUnit	2,443,130	2%
7	CVE-2017-9791	Remote code execution in (Apache Struts 1)	2,367,843	1%
8	CVE-2021-40438	Server Side Request Forgery (SSRF) in Apache HTTP Server	2,311,332	1%
9	CVE-2015-8562	PHP object injection in Joomla	1,716,435	1%
10	CVE-2013-2251	Remote code execution in (Apache Struts 2)	1,261,958	1%

Dominance of API Security in the Bug Bounty Landscape

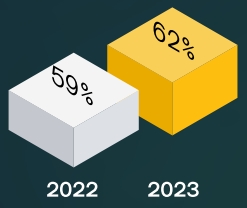
In 2023, the bug bounty landscape shifted significantly, with rewards for API vulnerabilities surpassing those for traditional web flaws. The report shows increased frequency and higher payouts for API issues, notably in Broken Access Control, Vulnerable/Outdated Components, and Injection vulnerabilities. API issues garnered 1.5 times more rewards than classic web vulnerabilities, and the average payout for API vulnerabilities was 65% higher, emphasizing the growing focus on API security.

A01 Broken Access Control	$46,125
A06 Vulnerable and Outdated Components	$27,828
A03 Injection	$22,698

The majority of these bounties were allocated for addressing A01 Broken Access Control, A06 Vulnerable and Outdated Components, and A03 Injection vulnerabilities.



API bounties share



API bounties payout share

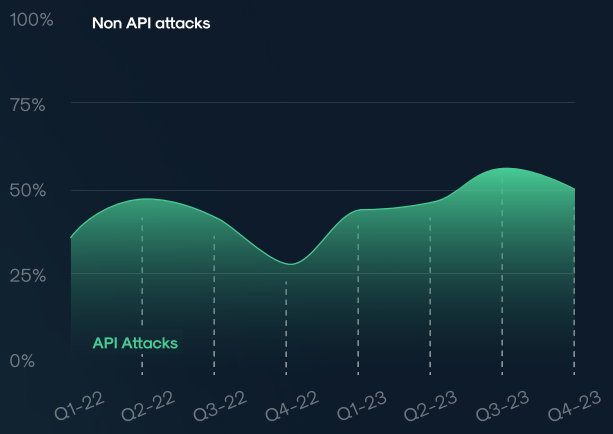
	Non API	API
Number of bounties	74	72
Total payouts	$98,010	$158,001
Highest payout	$5,000	$15,000
Average payout	$1,324	$2,194

Notably, API-related bounties are higher in value compared to other categories. The highest payout for an API bug was $15,000, which is three times larger than the highest non-API payout of $5,000.

In a recent analysis of bug bounty programs, it was found:

- Number of bounties was almost evenly split between API and non-API vulnerabilities, with 74 non-API and 72 API related,
- API-related vulnerabilities commanded significantly higher payouts, totaling $158,001, compared to $98,010 for non-API issues.
- Highest individual payouts, where the top API-related bounty reached $15,000, substantially more than the $5,000 for non-API.
- On average, each API-related bounty garnered $2,194, outpacing the average non-API payout of $1,324,
- This reflects the growing emphasis and value placed on API security.

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

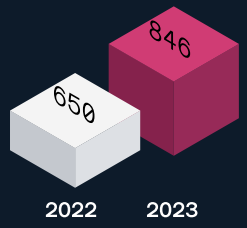


Change of API Bug Bounties Share by Quarter

API Vulnerability Landscape

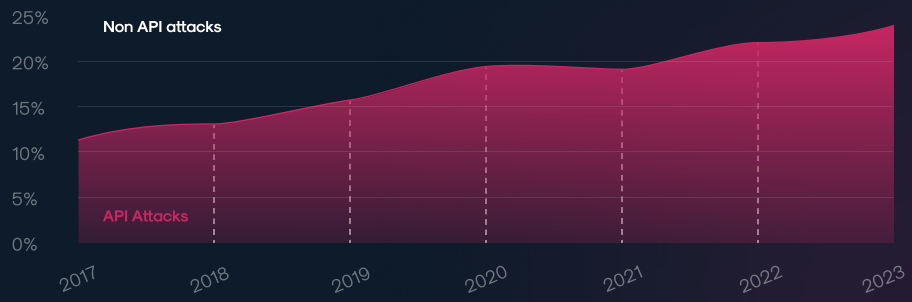
Increase in the Volume of API Vulnerabilities

In 2023, there was a notable 30% increase in API vulnerabilities compared to 2022, rising from 650 to 846.



Prominent Representation in The Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) Catalog

The CISA KEV catalog is an online database that catalogs security flaws and weaknesses in software applications. It includes vulnerabilities that have been exposed and exploited by attackers, providing a publicly accessible resource for the cybersecurity community. 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.



The change of API vulnerabilities share among CISA KEV catalog

Top exploited API-vulnerabilities

The report highlights a significant rise in API security threats, particularly focusing on the Log4Shell or Apache Log4j vulnerability (CVE-2021-44228). This high-severity issue, affecting the widely-used Apache Log4j 2 Java logging library, accounted for 33% of all detected CVEs, with over 52 million exploitation attempts.

The report points out the complexities in cyber risk management, especially given the ongoing issue of Log4Shell in 2023. This challenge is linked to the widespread use of Log4Shell in various Java-based applications, the intricacies involved in effectively managing patches, and the persistent targeting of this vulnerability by cyber attackers. The persistence of Log4Shell even into 2023, despite its earlier disclosure, highlights the ongoing struggle against evolving cybersecurity risks and the importance of proactive strategies in patch management and threat detection.

CVE-2021-44228

Name: Remote Code Execution in Apache Log4j (Log4shell)

Exploitation attempts: 52,457,688

Share of all detected CVE: 33%

API Leaks: A Growing Cybersecurity Concern

The ThreatStats™ report emphasizes the growing concern of API leaks as a central issue in the realm of cybersecurity. Key data and insights from the report include:

Prevalence and Impact of API Leaks:

The report highlights the rising concern of API leaks, emphasizing their continued threat. It points to significant data breaches at prominent companies such as Netflix, VMware, and SAP, illustrating the potential risks of API leaks. This growing trend underscores the importance of incorporating strong API leak prevention strategies into corporate security plans.

Frequency and Consequences of API Leaks:

The report underscores the growing issue of API leaks, marking them as persistent dangers. Notably, it cites recent serious data breaches at major firms like Netflix, VMware, and SAP as evidence of the risks associated with API leaks. This trend highlights the increasing need for robust API leak prevention measures as an integral part of corporate security planning.

Pre-Emptive Steps to Stop API Leaks:

Organizations must swiftly implement preventative measures to bolster protections against API leaks. Safeguarding APIs against potential breaches deserves immediate and proactive attention in business security plans as an integral component woven into security strategies from the start.

Get Ahead of API Vulnerabilities:

Companies need to take early, forward-thinking action to guard against API leaks, per the report's advice. It asserts that blocking API weaknesses cannot be an accessory to corporate defense blueprints, but instead warrants major emphasis up front.

Most Significant API Exploits

The most significant API Exploit

Highest H1 Payout for **Snapchat**: The most significant bug bounty payout in 2023.

The most notable API Exploit

Citrix Bleed (CVE-2023-4966): Most notable according to Google, involving a memory leak issue in Citrix Netscaler ADC, known for its comprehensive API security functionalities.

Most well-known API Exploit

Johnson OpenBlue Security Bug: Highlighted by CISA, this is the most well-known hardware API security bug of the year.

Research Methodology

The Annual API ThreatStats™ 2024 Report encapsulates a year's progress in understanding and combating API security threats. It builds upon the foundations laid by the quarterly reports of 2023, offers a comprehensive view of the evolving cybersecurity challenges and the strides made in API security. It is designed to inform and support security and application professionals by providing detailed data and analysis on API security trends. Its objective is to contribute to the broader understanding of cybersecurity challenges and aid in the development of more effective digital security strategies.

For the 2024 Annual ThreatStats™ report, our research methodology has been enhanced to include a more detailed analysis of API security vulnerabilities and can be broken down into three distinct areas as follows:

Vulnerability Classification

Our exhaustive analysis of API security vulnerabilities across multiple data sources was anchored by a multifaceted approach. This included both manual examination by security experts and analysis using Large Language Models (LLMs) to determine the relevance of an issue to API security, potentially resulting in a Common Weakness Enumeration (CWE) assignment. We further assessed each vulnerability's alignment with OWASP and OWASP API risks, followed by a manual reconciliation to iron out any inconsistencies between the two evaluations.

Vulnerability Scoring

We adopted a novel scoring technique that references Google's vulnerability score, derived from the volume of indexed pages citing each vulnerability by its CVE or other identifiers. This was complemented by cross-referencing with the CISA Known Exploited Vulnerabilities (KEV) catalog and a review of the Common Vulnerability Scoring System (CVSS) insights from original reports. Additionally, a ChatGPT-based analysis of the CVEs were performed for a more rounded assessment.

Extended Classification

To enhance our classification strategy, we utilized AI tools for an advanced grouping of vulnerabilities. We organized the issues by their CVSS ratings for each CWE category. Utilizing the ChatGPT 4 LLM, we accurately clustered these CWEs, effectively encompassing 99% of the API security vulnerabilities reported in 2023. This repetitive procedure allowed us to refine our categorizations and establish more precise and descriptive labels, thus improving our comprehension and classification of these vulnerabilities.

API Security Predictions 2024

The 2024 Wallarm ThreatStats™ Report contains information that enables us to foresee certain trends in API security that are likely to emerge over the course of 2024. By examining the statistics presented in this report, we can extrapolate several insights regarding the future direction of API security threats and safeguards expected to arise in the coming year.

1. **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 and 2025.

2. **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. 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.

3. **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.

4. **Rising 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.

5. **More APIs and more unmanaged APIs**
As the number of APIs in use increases, particularly in vital systems, so does the number of unmanaged or insufficiently monitored APIs, creating significant security blind spots. These unmanaged APIs are often vulnerable to attacks, as organizations might not even be aware of their existence or the threats they pose. “You can't protect what you can't see" underscores a critical cybersecurity challenge of you cannot safeguard what remains invisible to your organization.

6. **Persistent Exploitation of Log4j Vulnerability**
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.

7. **Increased Focus on Broken Access Control and Authorization Issues**
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.

8. **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.

9. **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.

10. **Emerging Trends: The Future of AI and Cybersecurity**
    - Increased AI integration: This will enhance threat detection and response, alongside a rise in sophisticated AI-driven cyber attacks, the cybersecurity landscape is poised for significant evolution.
    - Rise of AI-driven Cyber Attacks: As AI tools become more sophisticated, there will likely be a rise in AI-driven cyber attacks. Attackers may use AI to develop more advanced malware, phishing campaigns, and to exploit vulnerabilities more efficiently.

Wallarm Research Team
lab.wallarm.com

Book a demo at
request@wallarm.com

The report highlights the growing concern of API security threats, detailing the rise in vulnerabilities and the effectiveness of Wallarm in mitigating these risks. The report highlights the need for organizations to prioritize advanced API security measures and emphasizes the importance of staying ahead of evolving threats through proactive strategies. The report advocates for a holistic approach, emphasizing the need for ongoing updates to security protocols and fostering collaboration within the cybersecurity community.

Future initiatives should focus on a deeper analysis of API vulnerabilities, the improvement of security protocols, and the promotion of an ongoing learning and adaptive culture within cybersecurity practices.

For businesses seeking a comprehensive approach to API security challenges, Wallarm's solutions are pivotal. We cater to the holistic security needs of companies navigating the complexities of API threats. The ThreatStats™ report illustrates Wallarm's effectiveness in detecting and mitigating API vulnerabilities, highlighting its advanced threat response capabilities. This demonstrates Wallarm's vital role in enhancing cybersecurity strategies, especially against increasingly sophisticated digital threats. For businesses aiming to fortify their digital defenses, Wallarm offers a proven, robust solution to safeguard their critical digital infrastructure effectively.

www.wallarm.com

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