wallarm

Private APIs at Risk

Key findings from the Wallarm Quarterly API ThreatStats™ Report, Q1-2023

- Are your internal API-driven processes at risk?
- Are injection risks still the biggest type of real-world API vulnerabilities seen?
- Has the time-to-exploit continued to worsen?

THE WINTER OF OUR DISCONTENT

Still Sounding Our Stern Alarms

The initial take on API vulnerabilities published in Q1-2023 shows a slow rise in numbers and a relatively stable risk level (at High). But as always, there's more in the data than meets the eye. Read on to learn more!

KEY TAKE AWAYS

Three Things You Should Know

- Defending your internal infrastructure from API vulnerabilities continues to be job #1 – you must protect your crown jewels.
- Injection vulnerabilities continue to be the main attack vector for APIs – ignore them at your peril.
- Time-to-Exploit has shifted to the defenders' favor – but now isn't the time to relax.

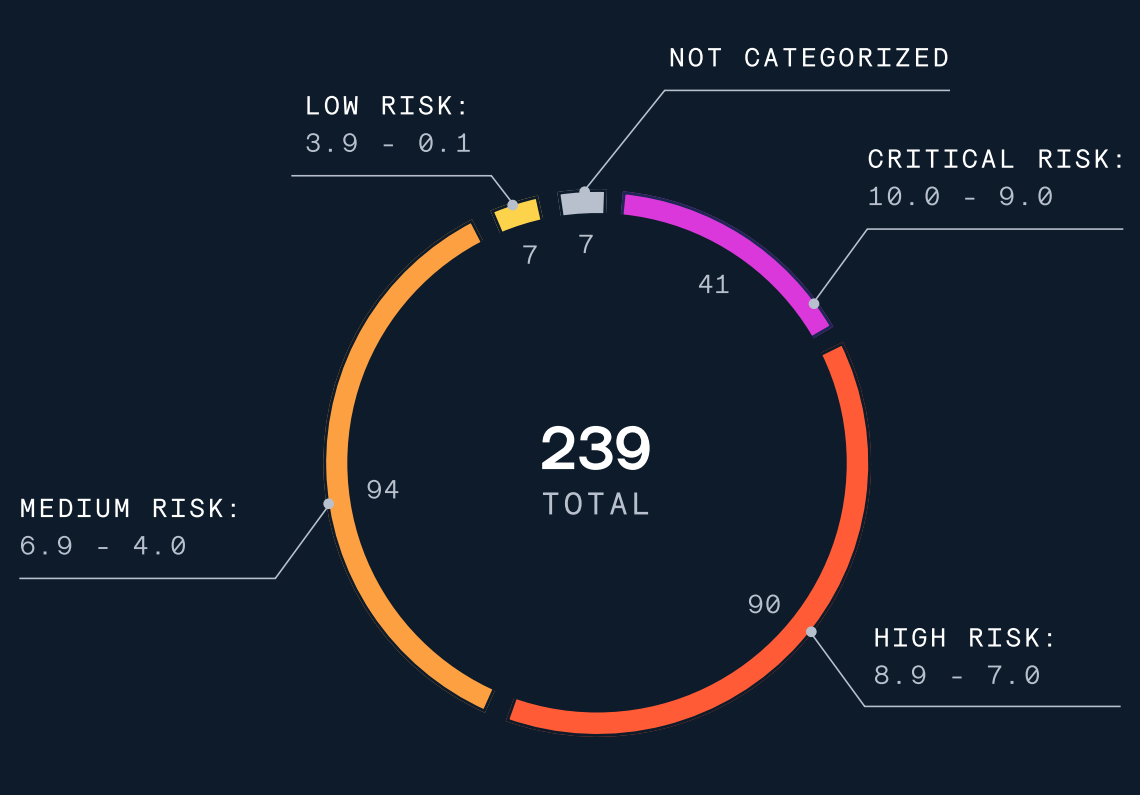
API VULNERABILITIES CONTINUE TO GROW

And the Risk Remains High

The number of API vulnerabilities analyzed in Q1-2023 continues to rise – up 12% from last quarter.

The average CVSS score in Q1 is 7.2 (High) – somewhat lower than in Q4-2022. But we should note that the median has held steady at 7.5 (High) since we started analyzing these data back in Q1-2022.

We do see a somewhat lower number of Critical & High vulnerabilities (55% vs. 57%), but it's too early to call this a trend.



Key Take Away #1

Protecting your internal infrastructure from API vulnerabilities continues to be job #1.

TOP-10 MOST IMPACTFUL API VULNERABILITIES

Are You Protecting the Soft Gooey Insides?

We are seeing the growing importance security of private APIs at companies. Q1-2023 saw a surge in top API security exploits targeting key components of internal processes, such as those recent in SAP NetWeaver AS for Java (CVE-2023-0017) and NVIDIA's graphics cards (CVE-2022-42279).

These vulnerabilities highlight the urgent need for tech-driven companies to prioritize securing their private APIs to protect valuable data and maintain business continuity.

CATEGORY: DEV TOOLS

Vendor	CVSSv3	Vulnerability	OWASP
RANCHER	CVSSv3: 9.8	CVE-2022-43755 Rancher Predictable cattle-token CWE-331 Insufficient Entropy	A02 OWASP API Top-10 API7 OWASP API Security Top-10
GitLab	CVSSv3: 9.8	CVE-2022-23739 An incorrect authorization vulnerability CWE-863 Incorrect Authorization	A01 OWASP API Top-10 API1 OWASP API Security Top-10
kubernetes	CVSSv3: 8.8	CVE-2022-3294 Kubernetes Node Address Isn't Always Verified When Proxying CWE-20 Improper Input Validation	A03 OWASP API Top-10 API8 OWASP API Security Top-10
HashiCorp	CVSSv3: 8.8	CVE-2023-1299 HashiCorp Nomad Job Submitter Privilege Escalation Using Workload Identity CWE-862 Missing Authorization	A01 OWASP API Top-10 API1 OWASP API Security Top-10
MINIO	CVSSv3: 8.8	CVE-2023-28434 MinIO Privilege Escalation CWE-269 Improper Privilege Management	A04 OWASP API Top-10 API1 OWASP API Security Top-10

CATEGORY: ENTERPRISE HW / SW

Vendor	CVSSv3	Vulnerability	OWASP
SAP NetWeaver	CVSSv3: 9.8	CVE-2023-0017 An unauthenticated attacker in SAP NetWeaver AS for Java CWE-284 Improper Access Control	A01 OWASP API Top-10 API1 OWASP API Security Top-10
NVIDIA	CVSSv3: 8.8	CVE-2022-42279 NVIDIA BMC SPX REST API OS Command Injection CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	A03 OWASP API Top-10 API8 OWASP API Security Top-10
GE	CVSSv3: 9.8	CVE-2022-43976 GE Grid Solutions: Directory Traversal Vulnerability in the Web Server CWE-no info	A07 OWASP API Top-10 API2 OWASP API Security Top-10
WAGO	CVSSv3: 9.8	CVE-2022-45138 WAGO - Multiple vulnerabilities in web-based management of multiple products CWE-306 Missing Authentication for Critical Function	A07 OWASP API Top-10 API2 OWASP API Security Top-10

CATEGORY: CLOUD PLATFORMS

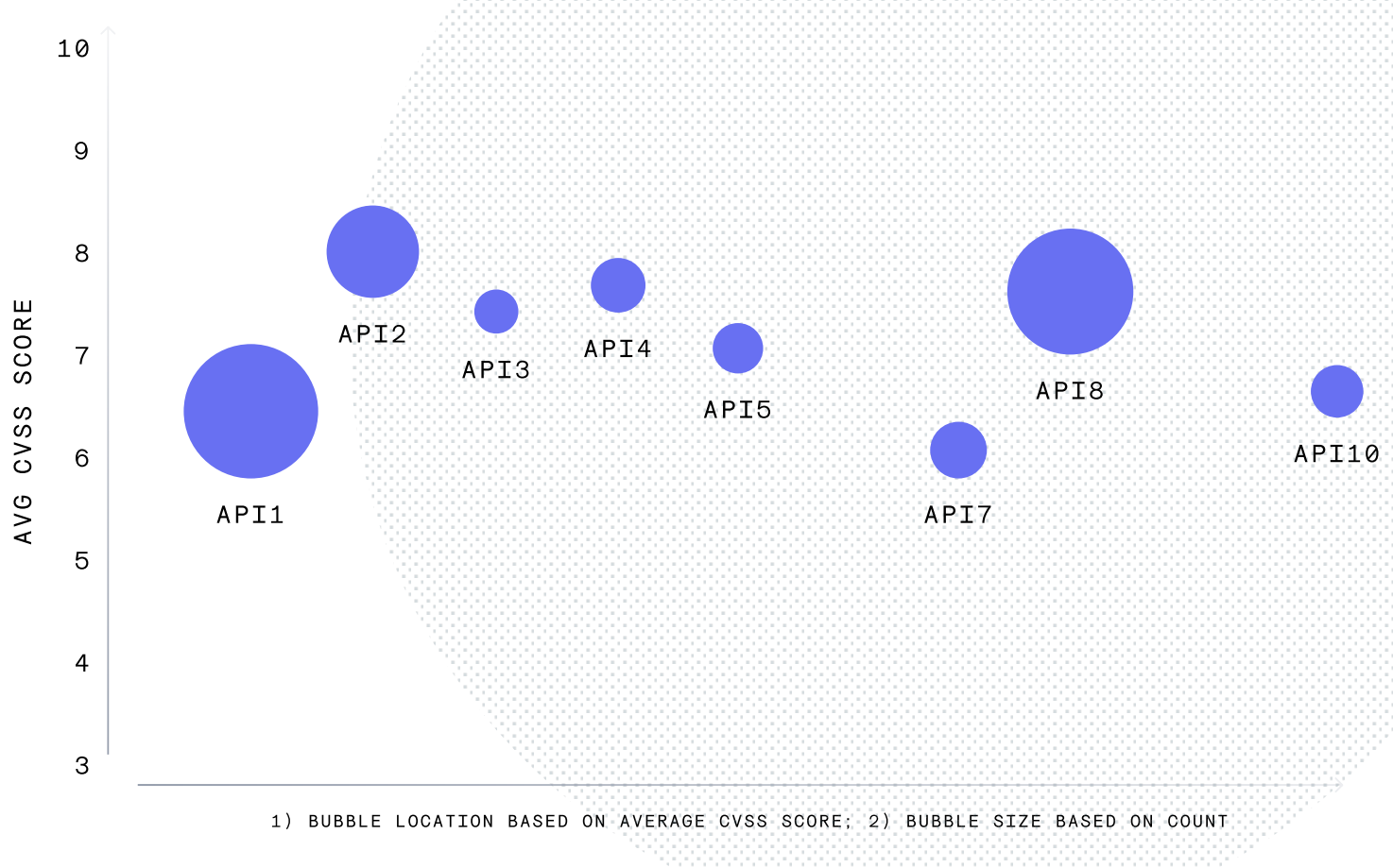
Vendor	CVSSv3	Vulnerability	OWASP
f5	CVSSv3: 8.5	CVE-2023-22374 BIG-IP iControl SOAP Format String Vulnerability CWE-134 Use of Externally-Controlled Format String	A01 OWASP API Top-10 API1 OWASP API Security Top-10

OWASP APISEC TOP-10 2019 MAPPING

Which Categories Should You Look at First?

We are foregoing our usual look at how the two OWASP Top-10 lists compare. Instead, we focus the risk categories within OWASP APIsec Top-10 (2019).

This quarter's mapping of vulnerability data shows that while API1: 2019 (BOLA) has the largest count, API8: 2019 (Injection) comes to the fore when the average CVSS score is factored in.[1]



OWASP APISEC TOP-10 2023 (RC) MAPPING

Are You Prepared for the Changes?

We also explored what the distribution of Q1-2023 vulnerabilities might look like when mapped against the newly proposed OWASP API Security Top-10.

Based on associated CWEs, we are not surprised to see that API10: 2023 (RC), Unsafe Consumption of APIs, garners the vast majority of the vulnerabilities disclosed in Q1-2023. This because it (somewhat controversially) contains CWEs associated with Injections.

Watch our on-demand webinar to learn more about the proposed OWASP APIsec Top-10 2023 (RC) and how it will impact your API vulnerability management program.

API1	BROKEN OBJECT LEVEL AUTHORIZATION (BOLA)	11%
API2	BROKEN AUTHENTICATION	6%
API3	BROKEN OBJECT PROPERTY LEVEL AUTHORIZATION	0%
API4	UNRESTRICTED RESOURCE CONSUMPTION	11%
API5	BROKEN FUNCTION LEVEL AUTHORIZATION (BFLA)	6%
API6	SERVER SIDE REQUEST FORGERY (SSRF)	9%
API7	SECURITY MISCONFIGURATION	9%
API8	LACK OF PROTECTION FROM AUTOMATED THREATS	0%
API9	IMPROPER INVENTORY MANAGEMENT	0%
API10	UNSAFE CONSUMPTION OF APIS	49%

[1] Based on the methodology used by MITRE to assess CWEs using (normalized frequency) x (normalized CVSS avg); for more on this approach, see https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25_supplemental.html#methodDetails

INJECTION VULNERABILITIES STILL RULE

The Achilles Heel of APIs

28% of the 61 unique CWEs seen this quarter are injection-related, accounting for 117 (45%) of all vulnerabilities assessed.

Of these, CWE-79 (XSS) leads the pack, followed by CWE-89 (SQLi) and CWE-863 (GraphQL Mutation).

Interestingly, CWE-918 (SSRF) – which is categorized API6 in the proposed OWASP APIsec 2023 list – lags behind in 9th place.

Key Take Away #2

Protecting against Injection attacks continues to be one of the main findings from API vulnerability reports – ignore them at your peril.

NUMBER	DESCRIPTION	PCT
CWE-79	Cross-site scripting	22%
CWE-89	SQL Injection (SQLi)	16%
CWE-863	GraphQL Mutation	15%
CWE-862	Missing Authorization (SQLi)	9%
CWE-22	Remote Code Execution (RCE)	8%
CWE-20	Improper Input Validation	5%
CWE-78	OS Command Injection	4%
CWE-295	Improper Certificate Validation	3%
CWE-918	Server-Side Request Forgery (SSRF)	3%
CWE-732	Incorrect Permission Assignment	3%
CWE-94	Code Injection	3%
CWE-611	XML Injection	3%
CWE-74	Injection	2%
CWE-434	Unrestricted File Upload	2%
CWE-502	Deserialization of Untrusted Data	2%
CWE-80	Basic XXS	1%
CWE-134	Use of Externally-Controlled Format String	1%

Key Take Away #3

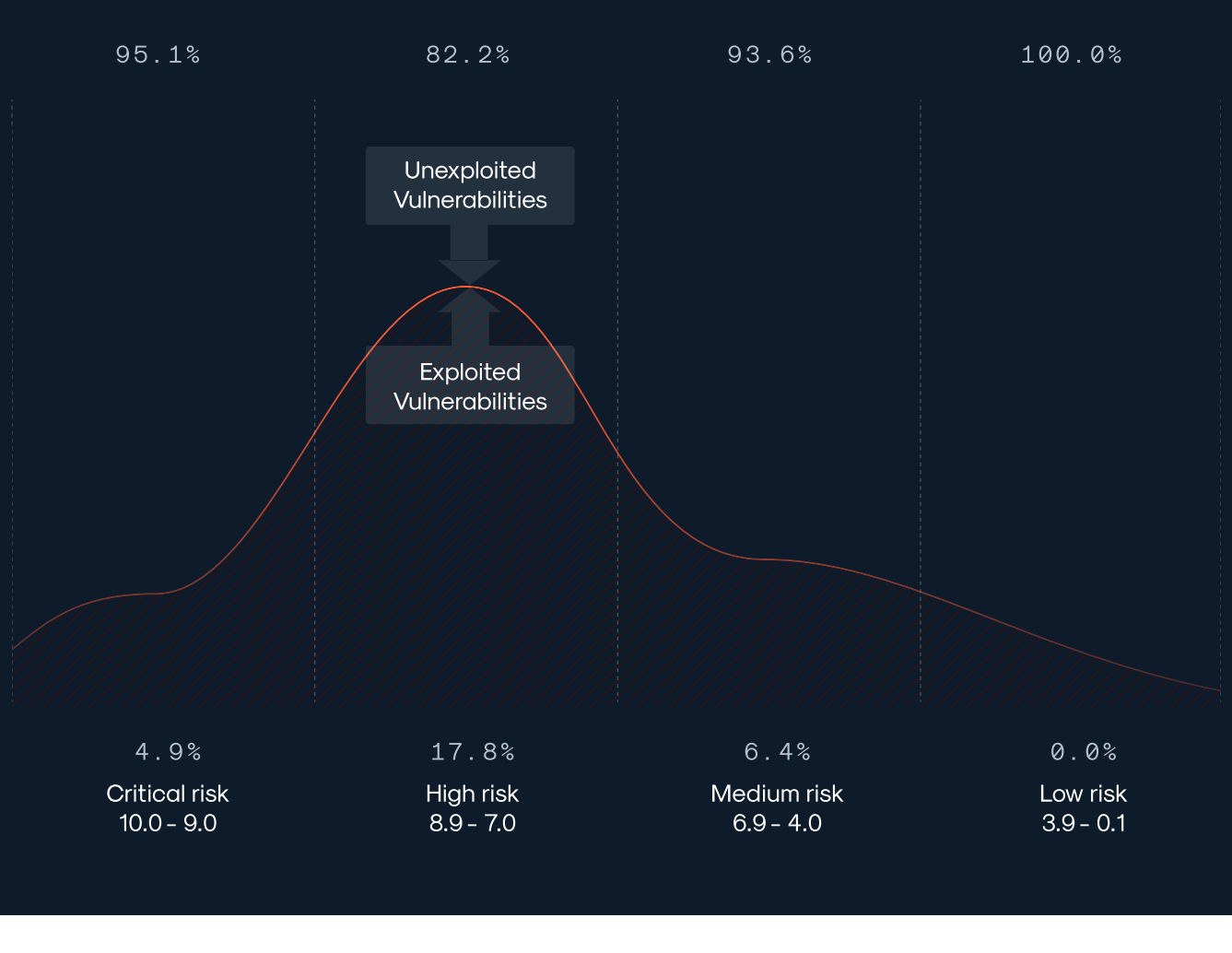
11 is the average number of days defenders have between vulnerability and associated exploit.

TIME-TO-EXPLOIT IMPROVES

Better, but Still Not Good

This quarter saw fewer published exploits (24 in Q1-2023 vs. 65 in Q4-2022) and some relief for defenders as the average time-to-exploit improved to +11 days (vs. -3 days in Q4-2022).

Most vulnerabilities which saw published exploits fell in the High range (CVSS score between 8.9 and 7.0), continuing the trend from Q4-2022.



ASSESSING YOUR API SECURITY

Put Real-World API Vulnerability Data to Work for You

While the Q1-2023 API vulnerabilities continued the slow & steady growth seen throughout most of 2022, our deeper analysis reveals three (3) key take-aways which have big implications on your API security programs.

- Defending your internal infrastructure from API vulnerabilities continues to be job #1 – you must protect your crown jewels. As we've said before, a much wider blast radius is likely if your internal APIs are exploited.
- Injection vulnerabilities continue to be the main attack vector for APIs – ignore them at your peril. And as we've said before, all the variants seen will require extra attention and remediation effort.
- Time-to-Exploit has shifted to the defenders' favor – but now isn't the time to relax. Consider the consequences if the sensitive data – including your proprietary IP or your customers' PII – are pwned from your internal, partner and/or public-facing APIs.

METHODOLOGY

We investigated API vulnerabilities that were publicly disclosed in Q1-2023, and the types of software vendors involved.

We also analyzed publicly disclosed exploit POCs to determine where the risk lies.

We mapped these issues across industry standards, including both OWASP Top-10 (2021) for web apps and OWASP API Security Top-10 (2019), CVSS scores, and CWEs.

Data is collected continuously throughout the year; this snapshot for the Q1-2023 data was taken on 04/07.

Use this data both to assess your exposure and to reduce the risk in your API portfolio.

WANT TO LEARN MORE ABOUT API VULNERABILITIES AND EXPLOITS?

Join your peers in the LinkedIn API ThreatStats group at linkedin.com/company/threatstats

Subscribe to our newsletter at lab.wallarm.com

Download the 2022 Year-End API ThreatStats™ Report at wallarm.com/resources/2022-year-end-api-threatstats-full-report

Watch the 2022 Year-in-Review webinar on-demand at wallarm.com/webinars/api-threatstats-2022-and-q4

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