wallarm

INFOGRAPHIC

Mind The API Time-To-Exploit Gap

Key findings from the Wallarm Quarterly API ThreatStats™ Report, Q4-2022

- Have API vulnerability remediation timelines gotten tighter?
- Do injections still account for a huge part of real-world API vulnerabilities?
- Do open source APIs contain more vulnerabilities than commercial products?

Another Relatively Quiet Quarter?

Maybe, But There Be Monsters Here!

The early analysis of Q4-2022 API vulnerabilities once again showed minimal change from the previous quarter:

- **Vulnerabilities** – up to 213 in Q4, from 203 in Q3 (+5% increase)
- **Vendors** – down to 122 in Q4, from 129 in Q3 (-5% decrease)
- **Critical & High rated vulnerabilities** – again holding steady at 57% of total

Does this mean we've survived the worst? No! Read on to learn more.

Key Take-Aways

Deeper analysis of the Q4 API vulnerabilities suggest your API security efforts have to run faster, but perhaps with a bit more direction.

Exploits – The time-to-exploit has now gone negative: on average, exploit POCs were published about three (3) days **before** the CVE is issued in Q4 – versus about four (4) days **after** in Q3. Clearly, proactive real-time protection is required.

Injection Vulnerabilities – This class of vulnerabilities (API8:2019) jumped to about 45% of all vulnerabilities in Q4 – the highest levels seen in 2022 – from about 34% in Q3. And because of all the variants, extra attention and remediation effort is required.

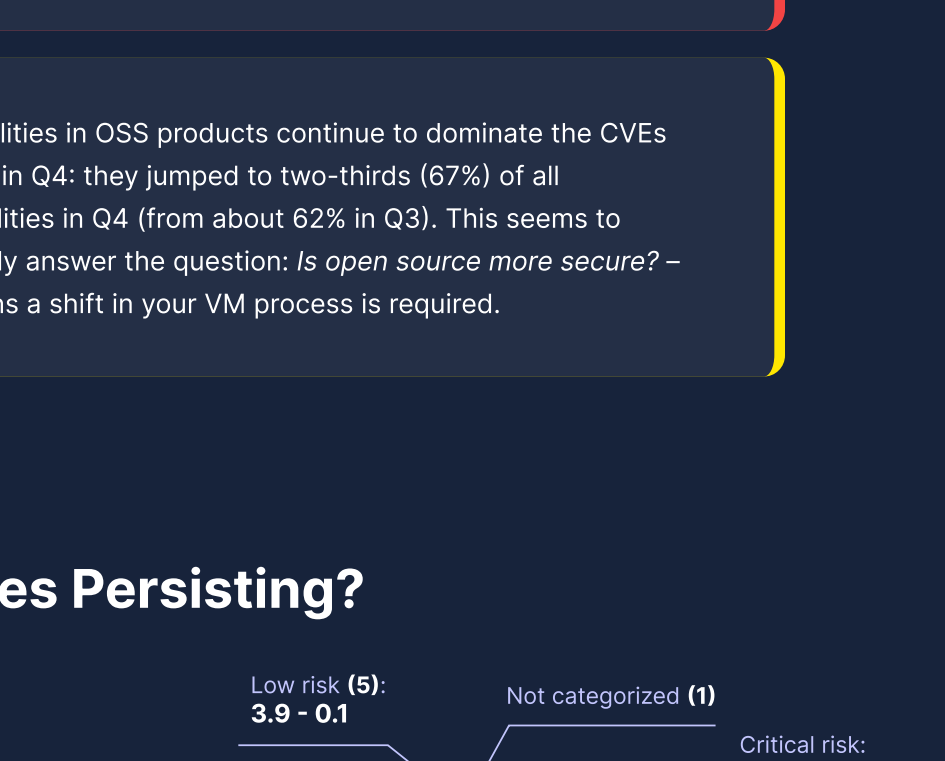
Open Source Software – Vulnerabilities in OSS products continue to dominate the CVEs analyzed in Q4: they jumped to two-thirds (67%) of all vulnerabilities in Q4 (from about 62% in Q3). This seems to definitively answer the question: *Is open source more secure?* – and means a shift in your VM process is required.

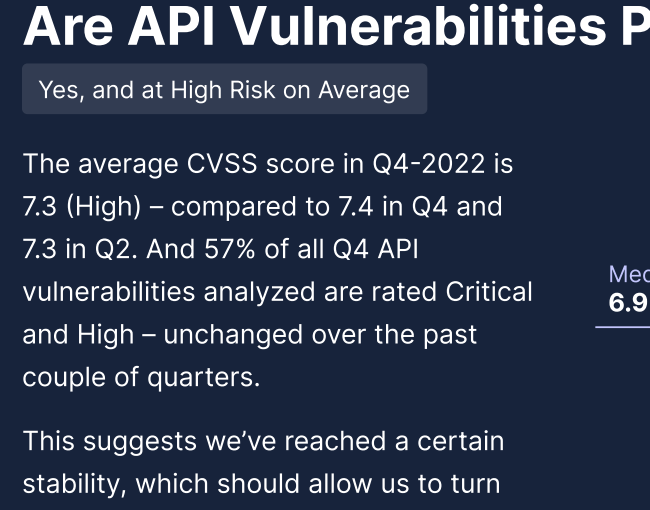
Are API Vulnerabilities Persisting?

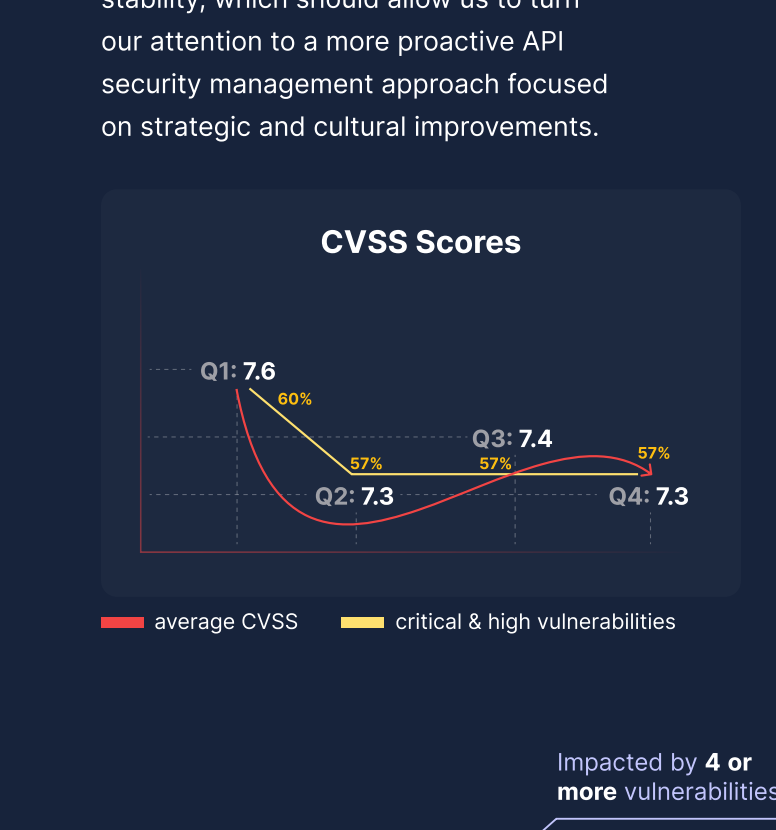
Yes, and at High Risk on Average

The average CVSS score in Q4-2022 is 7.3 (High) – compared to 7.4 in Q4 and 7.3 in Q2. And 57% of all Q4 API vulnerabilities analyzed are rated Critical and High – unchanged over the past couple of quarters.

This suggests we've reached a certain stability, which should allow us to turn our attention to a more proactive API security management approach focused on strategic and cultural improvements.







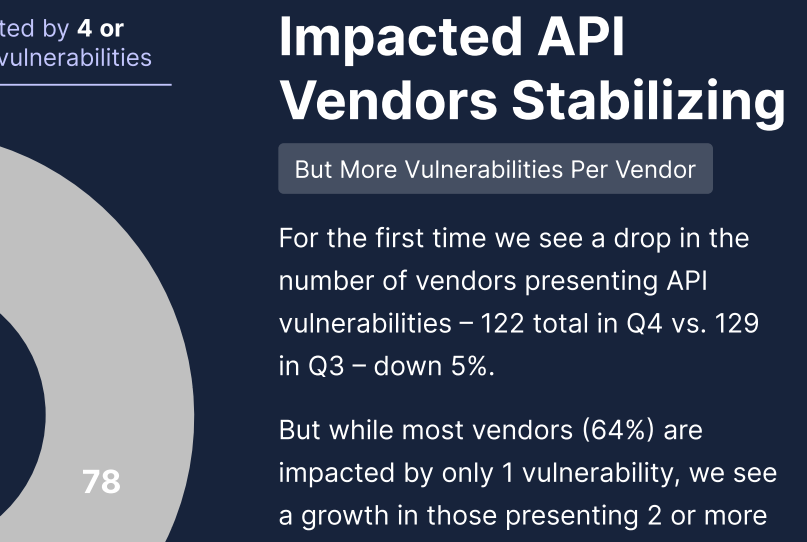
Impacted API Vendors Stabilizing

But More Vulnerabilities Per Vendor

For the first time we see a drop in the number of vendors presenting API vulnerabilities – 122 total in Q4 vs. 129 in Q3 – down 5%.

But while most vendors (64%) are impacted by only 1 vulnerability, we see a growth in those presenting 2 or more vulnerabilities – 36% in Q4 vs. only 27% in Q3.

This suggests your VM efforts can be a bit more focused, with an average of 1.7 API vulnerabilities per vendor in Q4.



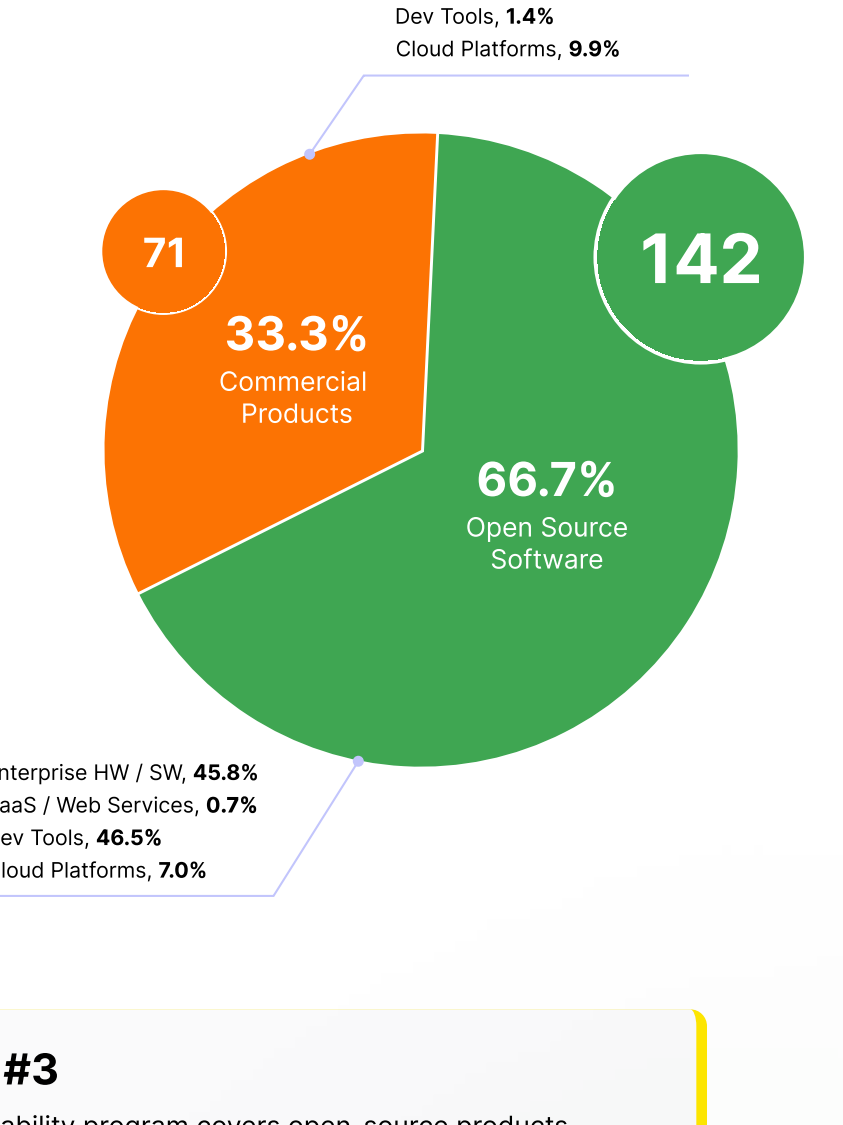
Are OSS Vulnerability Counts Growing?

Not Only More, But More Targeted

As we've seen each quarter this year, API vulnerabilities in open-source products continue to overshadow those in commercial products.

Two-thirds (67%) of all Q4 API vulnerabilities analyzed came from OSS products. Interestingly, we see a convergence in the Dev Tools and Enterprise HW / SW categories at about 46% each – as opposed to the commercial realm where Enterprise HW / SW clearly monopolize the API vulnerability landscape.

And, as seen last quarter, a majority of published exploit POCs focused on OSS products.



Key Take-Away #3

open source initiative

Make sure your API vulnerability program covers open-source products, especially those used in your development environment and buried in your SBOMs.

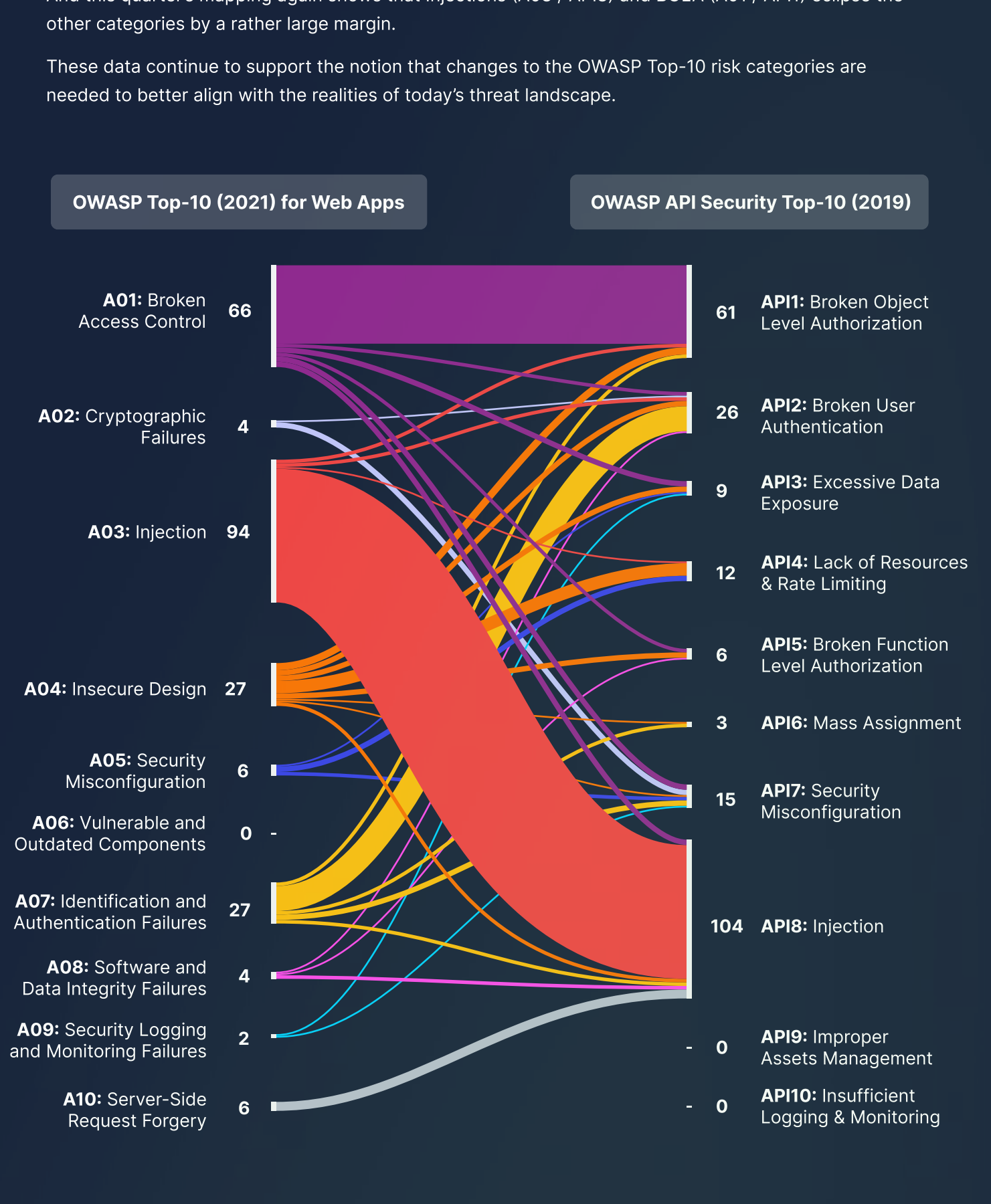
Which OWASP Top-10 Matters?

Less Signposts, More Guardrails

No Wallarm API ThreatStats™ report is complete without a look at how the OWASP risk categories compare. As usual, it's a higgledy-piggledy mass of cross references.

And this quarter's mapping again shows that Injections (A03 / API8) and BOLA (A01 / API1) eclipse the other categories by a rather large margin.

These data continue to support the notion that changes to the OWASP Top-10 risk categories are needed to better align with the realities of today's threat landscape.



Are Injections (Still) the Top Threat?

Yes, and in More Flavors Than You Imagined

In fact, Injection (A03 / API8) risks have cemented the title for most API vulnerabilities in 2022. But as seen in Q3, this broad category hides many variants – at least 19 different types of API injection vulnerabilities are found in the Q4 data.

These covered everything from Cross-Site Scripting (21% of all injection vulnerabilities) and SQLi (19%) to GraphQL Mutations and Prototype Pollution (both at 1%) – encompassing 18 different CWEs and each requiring different root-cause analysis and remediation.

Type	pct
Cross-Site Scripting (XSS)	21%
SQLi	19%
Denial of Service (DoS)	12%
Stored XSS	12%
Remote Code Execution	7%
Command Injection	6%
Server-Side Request Forgery (SSRF)	6%
GraphQL Mutations	1%
Code Execution	1%
Code Injection	1%
Deserialization	1%
Folder Creation	1%
Header Injection	1%
Local File Inclusion (LFI)	1%
Open Redirect	1%
OS Command Injection	1%
Prototype Pollution	1%
Script Injection	1%
Time-based SQLi	1%
not classified	5%

Key Take-Away #2

Injections

Injection risks continue to be the greatest threat vector – and the many variations seen in Q4 will require extra attention and effort to remediate.

How Long Before Exploit POCs Are Published?

Time-to-Exploit in Q4 Was ... Before You Heard About It

In Q4, we found exploit POCs were disclosed for over 30% of all published API vulnerabilities analyzed – more than double what was seen in Q3.

Equally troubling is that the time-to-exploit in Q4 has gone negative – averaging 3 days before the CVE is issued – a worrying continuation of the trend seen to date. And the timeline has grown to an astonishing 879 days (hopefully just a black swan sighting).

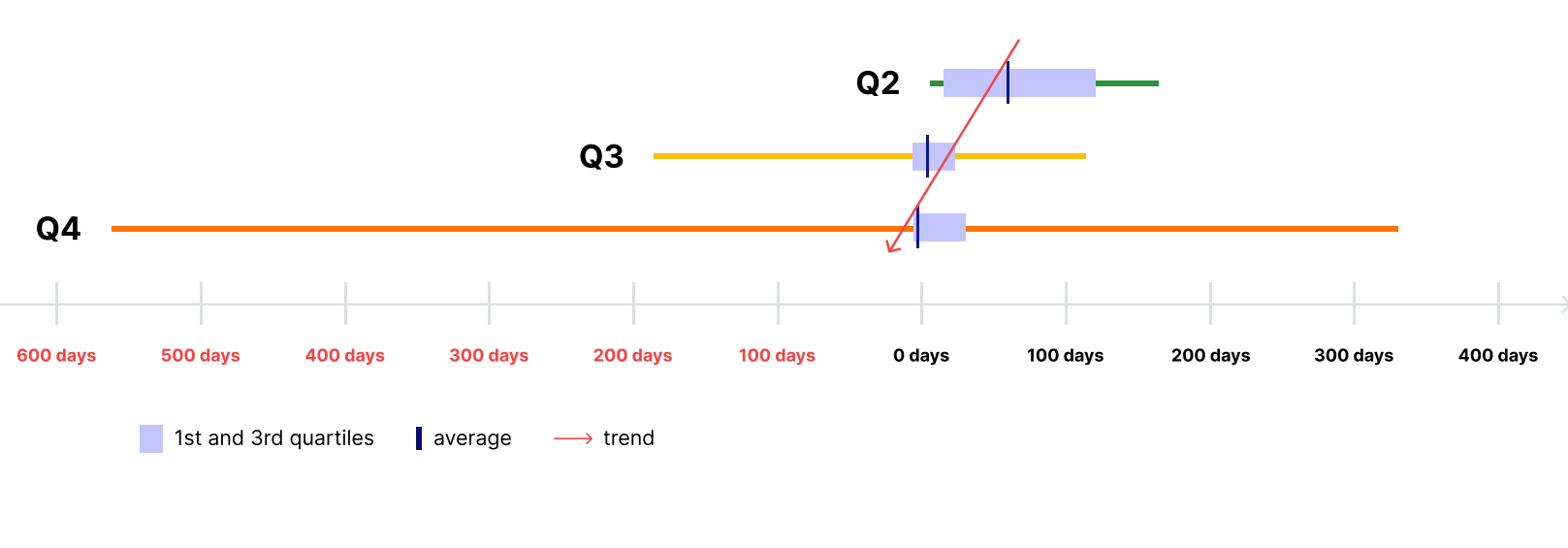
Key Take-Away #1

Exploits

Make sure your API VM program focuses on vulnerabilities which are being or have a likelihood of being exploited – and be prepared for more fire drills.

57% of all exploit POCs (37) were published an average of **64 days before** the CVE was published in Q4

43% of all exploit POCs (28) were published an average of **77 days after** the CVE was published in Q4



Most Impactful API Vulnerabilities

Do These Hit Home for You?

We assess these to be the most impactful API vulnerabilities published in Q4-2022, primarily due to the impact on your development and delivery infrastructure.

Category: Dev Tools

Vulnerability	CVSS	OWASP
GitLab CVE-2022-2992 Authenticated Remote Command Execution in Gitlab via GitHub import CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')	CVSSv3: 9.9 Exploit POC Published	A03 OWASP API Top-10 API8 OWASP API Security Top-10
Apache CVE-2022-42889 Text4shell Apache Commons Text RCE Vulnerability CWE-94 Code Injection	CVSSv3: 9.8	A03 OWASP API Top-10 API8 OWASP API Security Top-10
HASURA CVE-2022-46792 Hasura GraphQL Engine Missing Authorization Vulnerability CWE-732 Incorrect Permission Assignment for Critical Resource	CVSSv3: 8.8	A01 OWASP API Top-10 API1 OWASP API Security Top-10
CVE-2022-4223 pgAdmin Server Unauthenticated RCE while validating the binary path CWE-94 Code Injection	CVSSv3: 8.8	A03 OWASP API Top-10 API8 OWASP API Security Top-10
Grafana CVE-2022-31130 Grafana Data Source and Plugin Proxy Endpoints Leaking Authentication Tokens to Some Destination Plugins CWE-200 Exposure of Sensitive Information to an Unauthorized Actor, CWE-522 Insufficiently Protected Credentials	CVSSv3: 7.5	A01 OWASP API Top-10 API1 OWASP API Security Top-10
GitLab CVE-2022-3018 Information Exposure in GitLab CWE-668 Exposure of Resource to Wrong Sphere	CVSSv3: 4.9	A01 OWASP API Top-10 API1 OWASP API Security Top-10
GitLab CVE-2022-3325 Improper access control in GitLab CE/EE API CWE-732 Incorrect Permission Assignment for Critical Resource	CVSSv3: 4.3	A01 OWASP API Top-10 API1 OWASP API Security Top-10

Category: Enterprise HW / SW

Vulnerability	CVSS	OWASP
FORTINET CVE-2022-40684 FortiOS, FortiProxy, and FortiSwitchManager Authentication Bypass Vulnerability CWE-306 Missing Authentication for Critical Function	CVSSv3: 9.8 Exploit POC Published	A07 OWASP API Top-10 API2 OWASP API Security Top-10
StarWind CVE-2022-23858 REST API vulnerability in StarWind products NVD-CWE-noninfo	CVSSv3: 8.8	A07 OWASP API Top-10 API2 OWASP API Security Top-10
CVE-2022-43776 SSRF in Metabase GeoJSON URL CWE-918 Server-Side Request Forgery (SSRF)	CVSSv3: 6.5	A10 OWASP API Top-10 API8 OWASP API Security Top-10

Assessing Your API Security

Putting API Vulnerability Data to Work for You

While the Q4-2022 API vulnerabilities continued the slow & steady growth seen in Q3-2022, a deeper analysis reveals several key findings.

Key Take-Aways

These three (3) main findings have big implications on your API security programs.

Exploits – The time-to-exploit has now gone negative: on average, exploit POCs were published about three (3) days **before** the CVE is issued in Q4 – versus about four (4) days **after** in Q3. Clearly, proactive real-time protection is required.

Injection Vulnerabilities – This class of vulnerabilities (API8:2019) jumped to about 45% of all vulnerabilities in Q4 – the highest levels seen in 2022 – from about 34% in Q3. And because of all the variants, extra attention and remediation effort is required.

Open Source Software – Vulnerabilities in OSS products continue to dominate the CVEs analyzed in Q4: they jumped to two-thirds (67%) of all vulnerabilities in Q4 (from about 62% in Q3). This seems to definitively answer the question: *Is open source more secure?* – and means a shift in your VM process is required.

Expanding your vulnerability management program to cover APIs will require visibility across your entire API portfolio, assessing and triaging vulnerabilities as they arise, and ensuring mitigations are implemented – both in the code and at run-time. Refer to the **API Security Tutorial** for more information.

Methodology

We investigated API vulnerabilities that were publicly disclosed in Q4-2022, 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 **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 Q4-2022 data was taken on 01/31.

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 https://www.linkedin.com/company/threatstats/

Subscribe to our newsletter at lab.wallarm.com

Download the Q3-2022 API ThreatStats™ Report at https://www.wallarm.com/resources/q3-2022-api-threatstats-full-report

Register to watch the 2022 Year-in-Review webinar on-demand at https://www.wallarm.com/webinars/api-threatstats-2022-and-q4

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