wallarm

INFOGRAPHIC

DevOps Tools & Infrastructure Under Attack

Key findings from the Wallarm Quarterly API ThreatStats™ Report, Q3-2022

- Where are we most likely to be attacked?
- What is the most common attack vector?
- How long do we have to patch API vulnerabilities?

Smooth Sailing? Or Just a Lull in the Storm?

And Beware the Kraken!

Initial analysis of Q3-2022 API vulnerabilities suggests things have abated since last quarter – all of the high-level metics show minimal to no change:

- **Vulnerabilities** – up to 203 in Q3 from 184 in Q2 (16% increase)
- **Vendors** – up to 129 in Q3 from 111 in Q2 (16% increase)
- **Critical & High rated vulnerabilities** – holding steady at 57% of total

BUT ... dig a little deeper in the data and we find that these still waters run deep.

Key Takeaways

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

Infrastructure – A vast majority of the most impactful vulnerabilities analyzed this quarter involved DevOps tools and infrastructure – which clearly **shifts your security focus.**

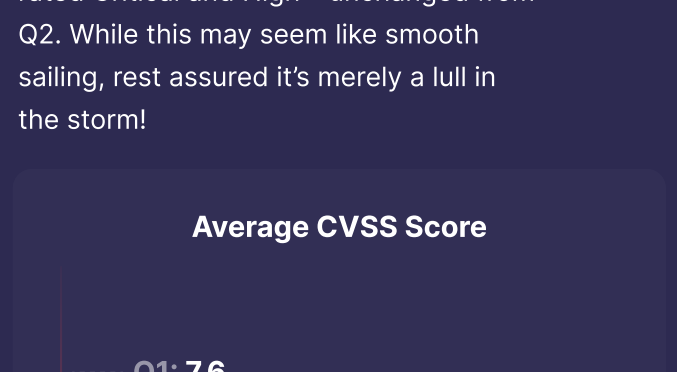
Injections – The OWASP Top-10 Injection categories (A03:2021 for web apps and API8:2019 for APIs) top the charts, but further inspection reveals many, many variations – **which undoubtedly requires extra effort to remediate.**

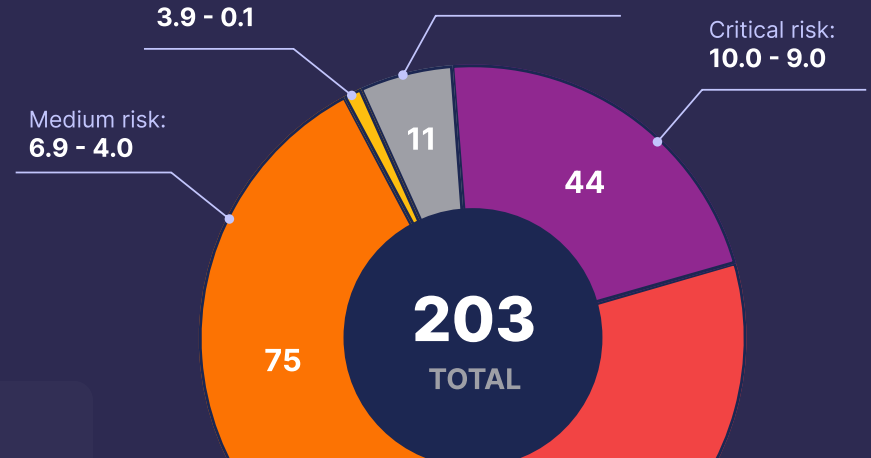
Exploits – We were a bit surprised to find the **average gap between CVE and exploit POC publication was zero days** (!) – which obviously impacts your mitigation timeline.

API Risks Remain High

Continued Vigilance Is Essential

The average CVSS score in Q3-2022 is 7.4 – compared to 7.3 in Q2. And 57% of all Q3 API vulnerabilities collected are rated Critical and High – unchanged from Q2. While this may seem like smooth sailing, rest assured it's merely a lull in the storm!





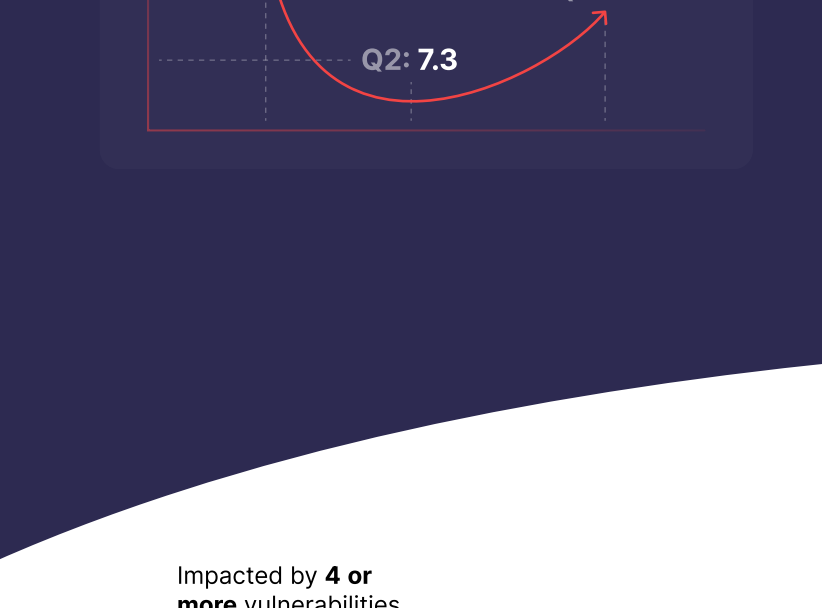
What's In Your Portfolio?

More Vulnerabilities Impacting More Vendors

As expected, this quarter did not see the huge increase in vendors impacted as seen last quarter – up only 16%, in line with CVEs analyzed.

And while a vast majority of vendors (73%) are impacted by only 1 vulnerability, we did find 8 vendors (6%) which were impacted by 4 or more vulnerabilities.

However, the devil – and impact on your APIs – is in the details.

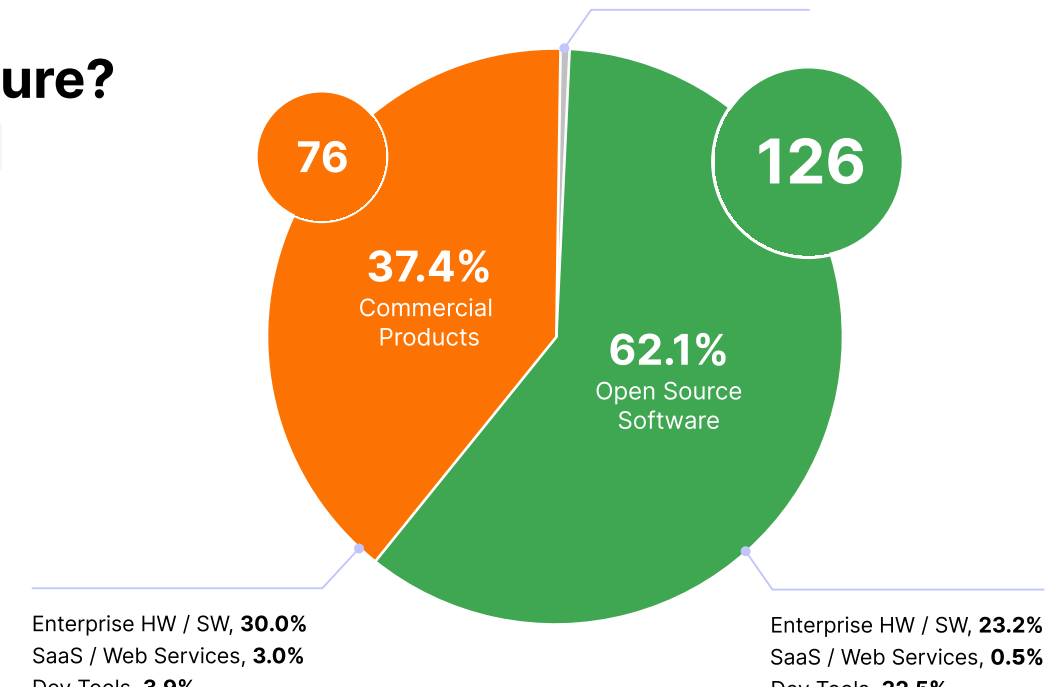


Is Open Source Really More Secure?

The Data Continue to Suggest No

Over 60% of reported vulnerabilities are related to Open Source software, with the remainder related to commercial products. Overall, the Dev Tools (which includes DevOps tools) and Enterprise HW / SW categories accounted for over 87% of the total.

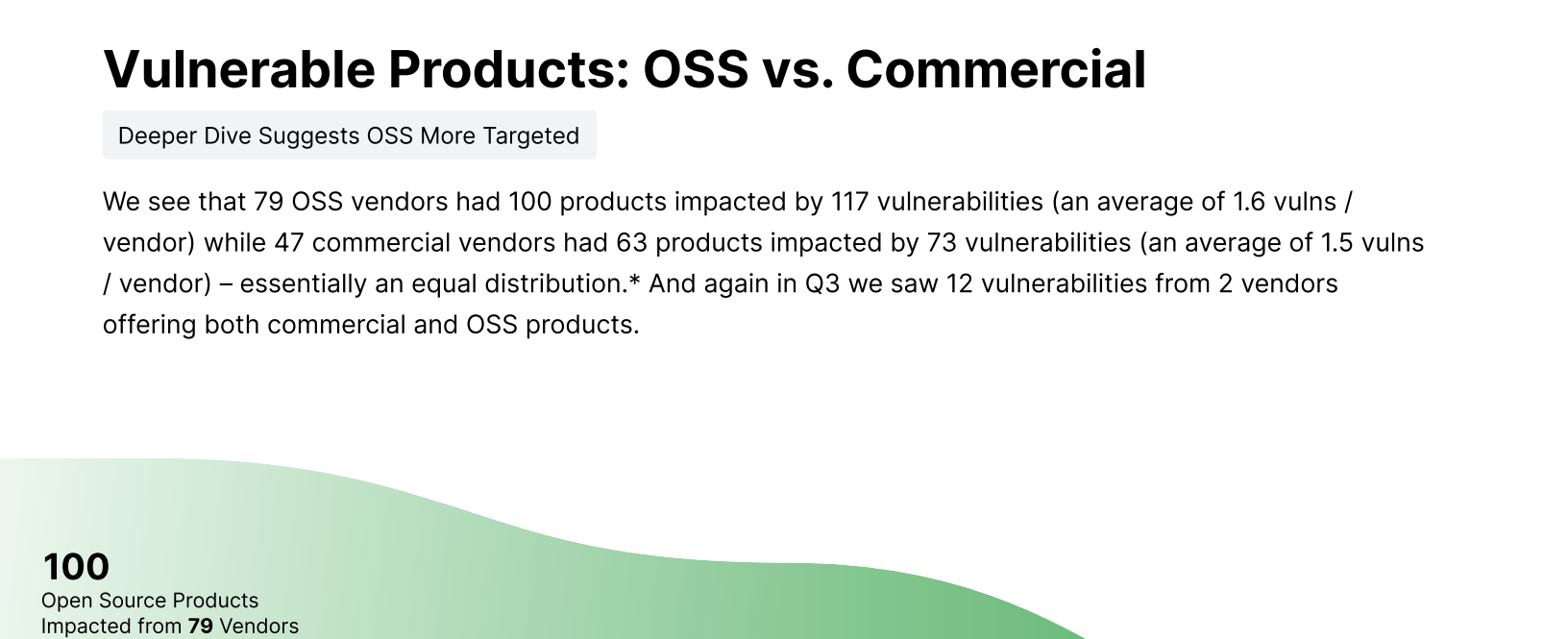
More worryingly, 80% of published exploit POCs were aimed at OSS products – not surprising, yet a good reminder.



Vulnerable Products: OSS vs. Commercial

Deeper Dive Suggests OSS More Targeted

We see that 79 OSS vendors had 100 products impacted by 117 vulnerabilities (an average of 1.6 vulns / vendor) while 47 commercial vendors had 63 products impacted by 73 vulnerabilities (an average of 1.5 vulns / vendor) – essentially an equal distribution.* And again in Q3 we saw 12 vulnerabilities from 2 vendors offering both commercial and OSS products.



* one vendor could not be classified and is not included in this analysis.

Key Take-Away #1 – **Infrastructure** – Make sure your API VM program covers internal tools, especially those with a likely large blast radius.

Most Impactful API Vulnerabilities

Infrastructure at Risk

We assess these to be the most impactful API vulnerabilities in Q3-2022, primarily due to impact on development and delivery infrastructure.

Category: DevOps Tools

Vendor	Vulnerability	CVSSv3	OWASP API Top-10	OWASP API Security Top-10
GitLab	CVE-2022-2884 GitLab Remote Command Execution **CWE-77:** Improper Neutralization of Special Elements used in a Command ('Command Injection')	9.9	A03	API8
RANCHER	CVE-2022-36783 Rancher - Failure to properly sanitize credentials in cluster template answers **CWE-312:** Cleartext Storage of Sensitive Information	9.9	A01	API1
argo	CVE-2022-31105 Argo CD Improper Certificate Validation **CWE-295** Improper Certificate Validation	9.6	A07	API2
Casdoor	CVE-2022-38638 Casdoor Arbitrary file write/overwrite Vulnerability **CWE-862:** Missing Authorization	9.1	A04	API8
Grafana	CVE-2022-31107 Grafana Account Takeover Via OAuth Vulnerability **CWE-863** Incorrect Authorization	7.5	A01	API1
HashiCorp	CVE-2022-41803 HashiCorp Consul Auto-Config JWT Authorization Missing Input Validation **CWE-862** Missing Authorization	7.1	A03	API8
GitLab	CVE-2022-1999 GitLab CE/EE Improper privilege Management **CWE-269:** Improper Privilege Management	5.3	A04	API1
kubernetes	CVE-2022-3172 Kubernetes Aggregated API server can cause clients to be redirected **CWE-918:** Server-Side Request Forgery (SSRF)	5.1	A10	API1
JFrog	CVE-2022-4668 JFrog Artifactory Sensitive Data Exposure **CWE-359:** JFrog Artifactory Sensitive Data Exposure	4.9	A01	API1

Category: Enterprise HW / SW

Vendor	Vulnerability	CVSSv3	OWASP API Top-10	OWASP API Security Top-10
APACHE	CVE-2022-25168 Apache Hadoop Arbitrary Commands Injection **CWE-88:** Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	9.8	A03	API8
FORTINET	CVE-2022-29060 FortiDDoS - Use of hardcoded key for the JWT token **CWE-321:** Use of Hard-coded Cryptographic Key	8.1	A02	API2
f5	CVE-2022-34851 BIG-IP and BIG-IQ iControl SOAP vulnerability **CWE-20** Improper Input Validation	6.5	A03	API8

Be On The Lookout for These Too

TIMTOWTDI

What to address first? Triaging vulnerabilities for mitigation can be based on a variety of criteria, including:

Ranking – Based on frequency and severity, much like how MITRE assesses CWEs[1]

Frequency – How many vulnerabilities are found in the vendor's products?

Severity – How bad are the vulnerabilities in a particular vendor's products?

Top-5 based on ranking (frequency x CVSS)

Vendor	count	CVSS avg
Red Hat	10	7.8
Cisco	6	7.6
Jenkins	8	6.1
Tabit Technologies	5	7.4
Harbor	5	6.6

Top-5 based on frequency (count)

Vendor	count	CVSS avg
Red Hat	10	7.8
Jenkins	8	6.1
Cisco	6	7.6
Zyxel	6	5.7
Tabit Technologies	5	7.4
Harbor	5	6.6
GitLab	5	5.7

Top vulnerabilities based on severity (CVSS average)

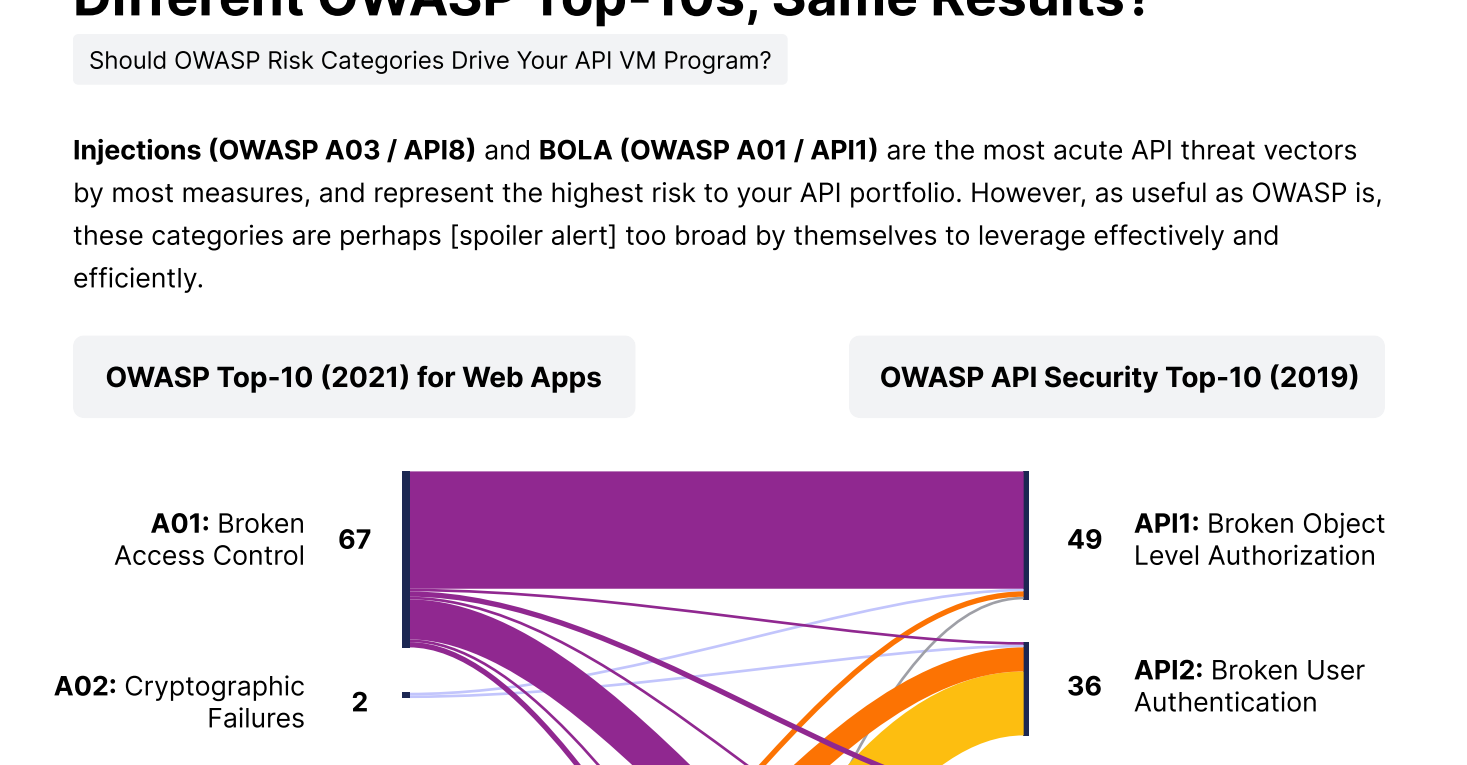
Vendor	count	CVSS avg
Rancher	2	9.9
AEB-labs	1	9.9
Carlo Gavazzi	2	9.8
miniOrange	2	9.8
Acrontum	1	9.8
Alfasado	1	9.8
Cloud Native Computing Foundation	1	9.8
dotCMS	1	9.8
dotnetcore	1	9.8
Eric Cornelissen	1	9.8
Jeecg	1	9.8
KubeVela	1	9.8
laverdet	1	9.8
MiCODUS	1	9.8
Peisheng Information	1	9.8
Poly	1	9.8
Six Apart	1	9.8
some-natalie	1	9.8
Transtek	1	9.8
unknown	1	9.8
Wavlink	1	9.8

[1] See https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25_supplemental.html#methodDetails

Different OWASP Top-10s, Same Results?

Should OWASP Risk Categories Drive Your API VM Program?

Injections (OWASP A03 / API8) and **BOLA (OWASP A01 / API1)** are the most acute API threat vectors by most measures, and represent the highest risk to your API portfolio. However, as useful as OWASP is, these categories are perhaps [spoiler alert] too broad by themselves to leverage effectively and efficiently.



Included: Most Dangerous CWEs

Bring Focus to Software Weaknesses

2022 CWE Top 25 Most Dangerous Software Weaknesses

Rank	ID	Q3 count*	Name
1	CWE-787	1	Out-of-bounds Write
2	CWE-79	27	Cross-site Scripting
3	CWE-89	7	SQL Injection
4	CWE-20	6	Improper Input Validation
5	CWE-125	1	Out-of-bounds Read
6	CWE-78	4	OS Comand Injection
7	CWE-416	n/a	Use After Free
8	CWE-22	15	Path Traversal
9	CWE-352	2	Cross-Site Request Forgery (CSRF)
10	CWE-434	1	Unrestricted Upload of a File with Dangerous Type
11	CWE-476	n/a	NULL Pointer Dereference
12	CWE-502	1	Deserialization of Untrusted Data
13	CWE-190	n/a	Integer Overflow or Wraparound
14	CWE-287	10	Improper Authentication
15	CWE-798	5	Use of Hard-coded Credentials
16	CWE-862	7	Missing Authorization
17	CWE-77	5	Command Injection
18	CWE-306	3	Missing Authentication for Critical Function
19	CWE-119	n/a	Memory Buffer Overflow
20	CWE-276	0	Incorrect Default Permissions
21	CWE-918	4	Server-Side Request Forgery (SSRF)
22	CWE-362	0	Race Condition
23	CWE-400	8	Incontrolled Resource Consumption
24	CWE-611	1	Improper Restriction of XML External Entity Reference
25	CWE-94	1	Code Injection

***n/a** means this CWE is **not** related to API Security; this quarter includes two not normally seen in APIs: CWE-787 and CWE-125.

Nearly 54% of the Q3 vulnerabilities analyzed referenced CWEs included in the 2022 CWE Top 25 Most Dangerous Software Weaknesses list from MITRE / CISA[2].

69 unique CWEs found in Q3 reports

19 of these are considered "most dangerous"

Most seen: CWE-79, CWE-22 and CWE-287

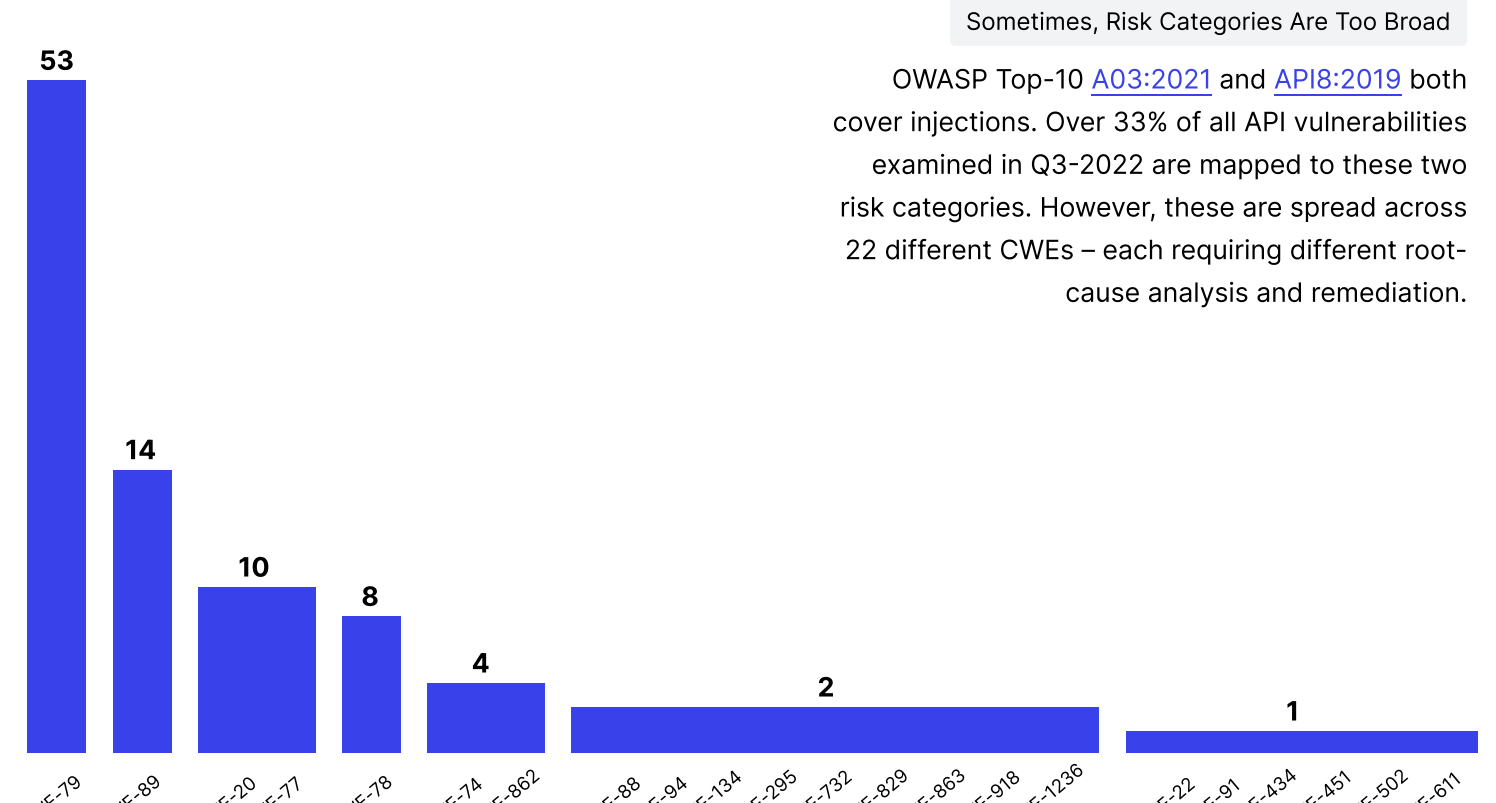
[2] https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

Key Take-Away #2 – **Injections** – Make sure your API VM program drills into each OWASP risk category to focus root cause & remediation.

We Have 22 Problems, All Called Injections

Sometimes, Risk Categories Are Too Broad

OWASP Top-10 A03:2021 and API8:2019 both cover injections. Over 33% of all API vulnerabilities examined in Q3-2022 are mapped to these two risk categories. However, these are spread across 22 different CWEs – each requiring different root-cause analysis and remediation.

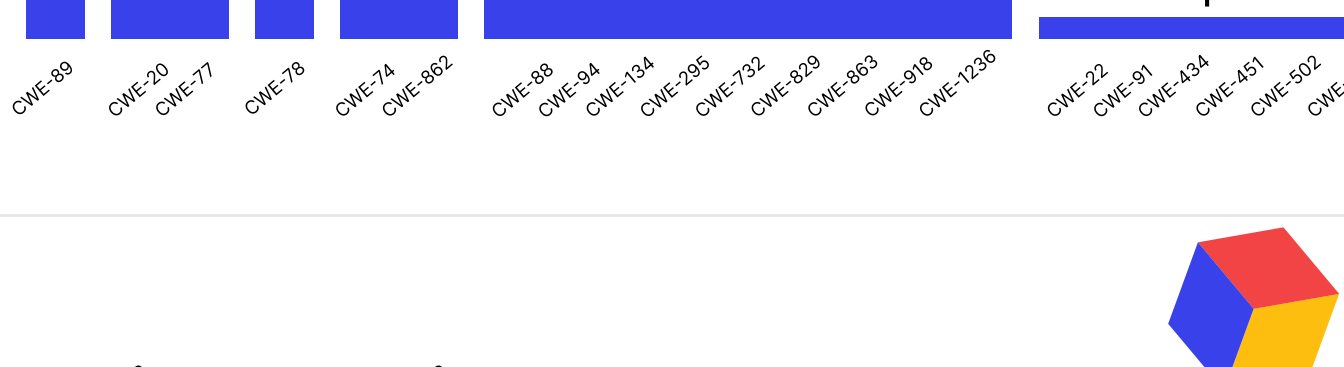


Published Exploit POCs

It's Not Just How Many, But When!

In Q3, we found exploit POCs were released for nearly 15% of the published API CVEs.

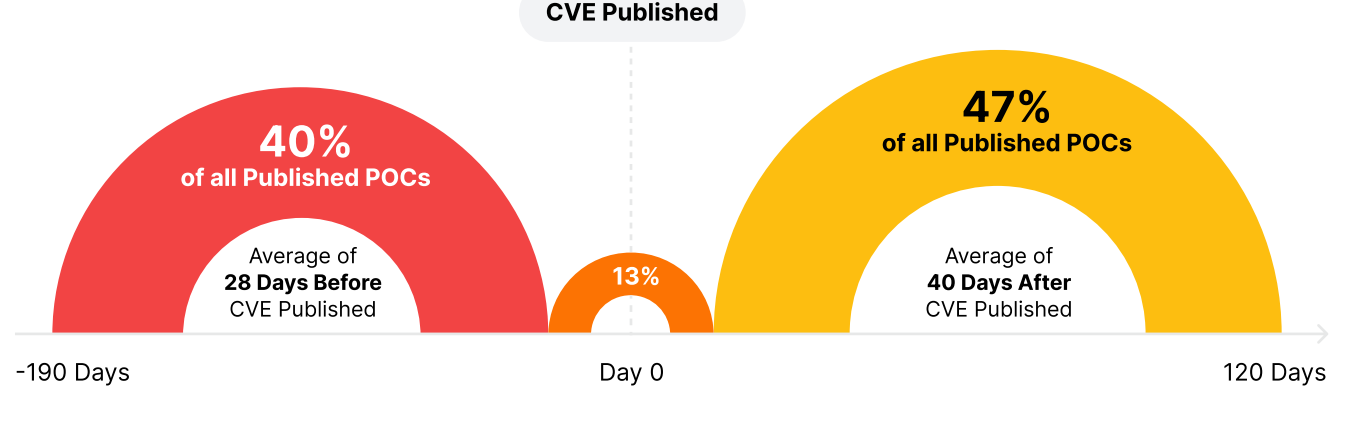
- 70% of exploited vulnerabilities vs. only 54% of unexploited CVEs are classified as critical or high risk
- The median gap between an exploit POC being published for a Q3 API CVE? Zero days!



Average Time-to-Exploit

More worryingly, in over 1/2 those cases, the POC was released before the CVE (aka 0-days) – an average of 28 days before!

Key Take-Away #3 – **Exploits** – Make sure your API VM program focuses on vulnerabilities being or have a high likely of being exploited.



Assessing Your API Security

Putting API Vulnerability Data to Work for You

Overview. While the Q3-2022 API vulnerabilities growth rate was not as spectacular as in Q2-2022, a deeper analysis revealed three (3) key take-aways.

Key Takeaways

Infrastructure – A vast majority of the most impactful vulnerabilities analyzed this quarter involved DevOps tools and infrastructure – which clearly **shifts your security focus.**

Injections – The OWASP Top-10 Injection categories (A03:2021 for web apps and API8:2019 for APIs) top the charts, but further inspection reveals many, many variations – **which undoubtedly requires extra effort to remediate.**

Exploits – We were a bit surprised to find the **average gap between CVE and exploit POC publication was zero days** (!) – which obviously impacts your mitigation timeline.

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 Q3-2022, 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 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 of the Q3-2022 data was taken on 10/18.

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 the LinkedIn 🔥 API security community 🔥 group at https://www.linkedin.com/groups/12624726/

Subscribe to our newsletter at lab.wallarm.com

Download the Q2-2022 API Vulnerability Report at https://www.wallarm.com/resources/q2-2022-api-vulnerability-exploit-full-report

Register to participate in the Q3-2022 API ThreatStats Report webinar at https://www.wallarm.com/webinars/q3-2022-api-threatstats

wallarm

Version v1.1, updated 11.02.2022

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