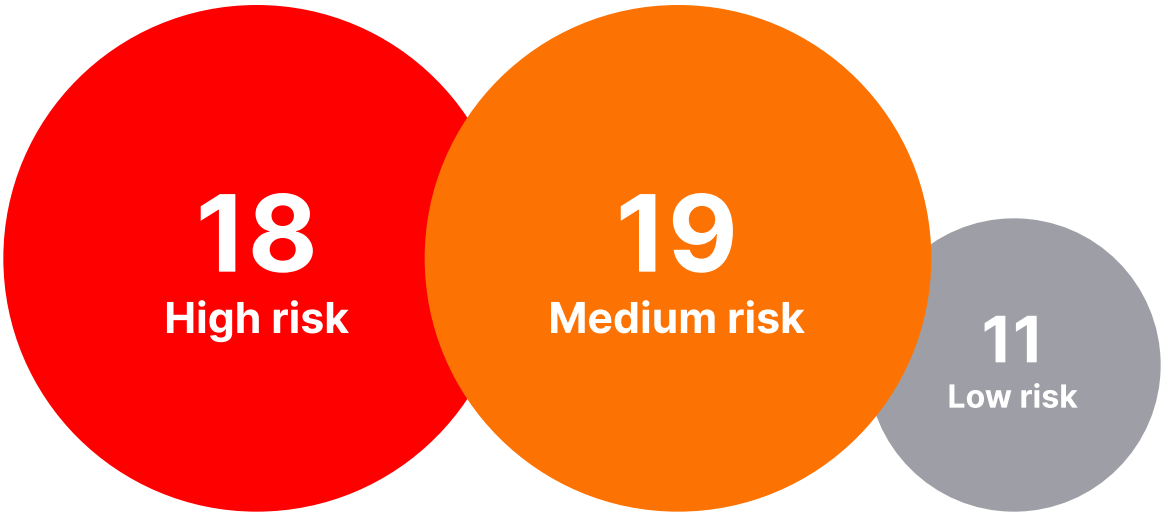
wallarm

WHITEPAPER

API Vulnerabilities Discovered And Exploited In Q1-2022



API Vulnerabilities Disclosed And Exploited In Q1-2022

This work is based on Wallarm research of API security issues and exploits that were publicly disclosed in Q1-2022. We explain what issues were found, and which vendors and products were affected. We map these issues across industry standards, including CWEs, CVEs, both OWASP Top-10 and OWASP API Security Top-10, and CVSS scores.

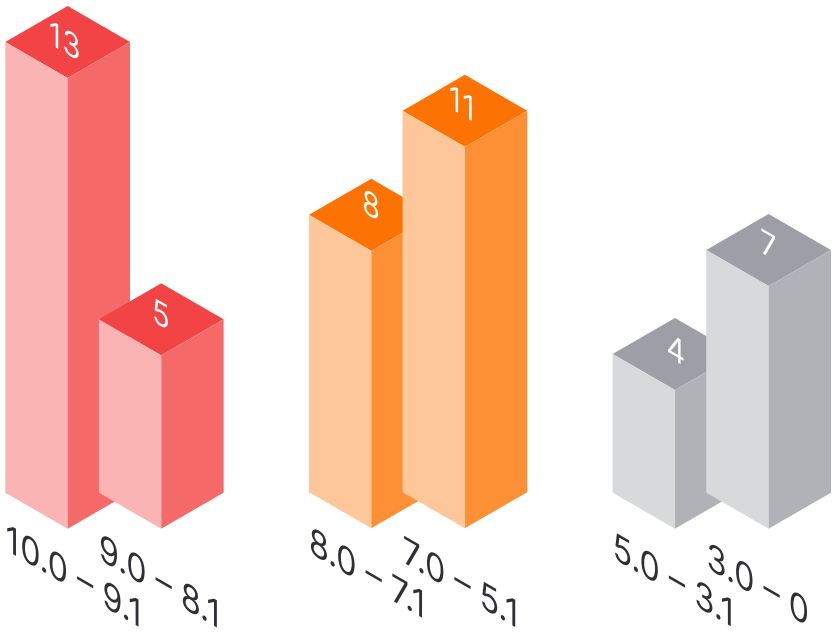
48
TOTAL

18
HIGH RISK

19
MEDIUM RISK

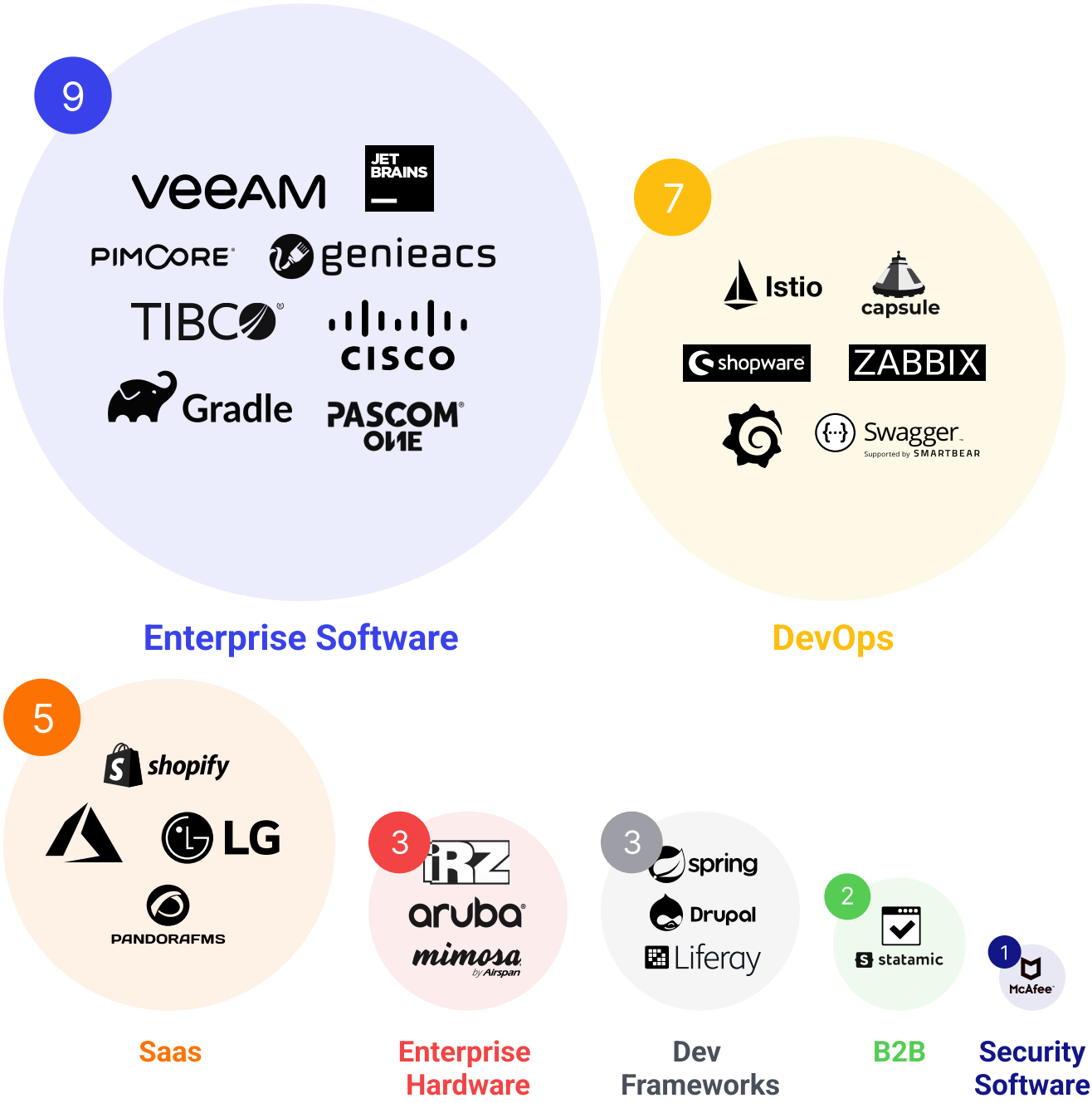
11
LOW RISK

CVSSv3 Score



30 Total Products Vulnerable

This work is based on Wallarm research of API security issues and exploits that were publicly disclosed in Q1-2022. We explain what issues were found, and which vendors and products were affected. We map these issues across industry standards, including CWEs, CVEs, both OWASP Top-10 and OWASP API Security Top-10, and CVSS scores



OWASP Heat Map

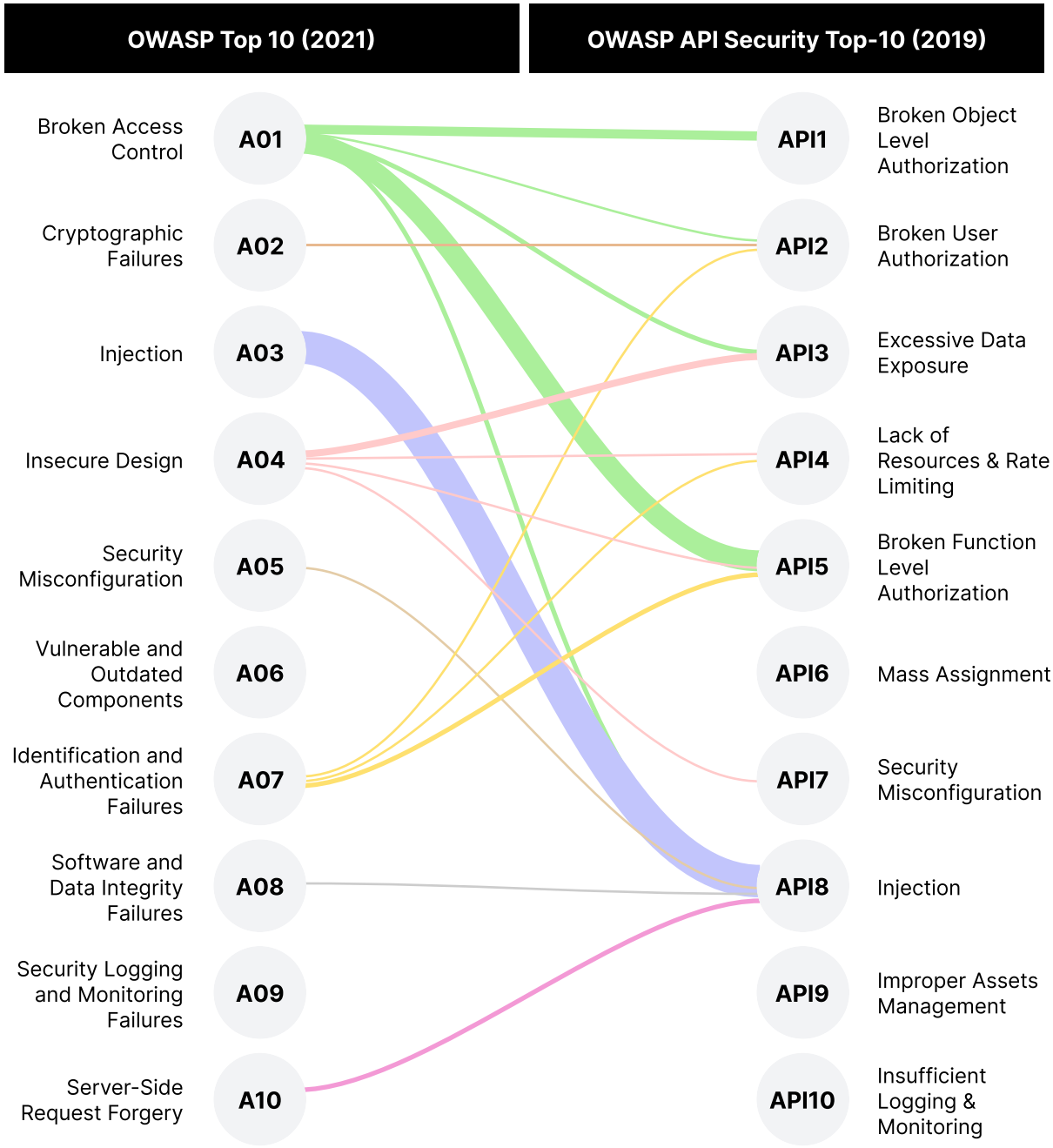
We mapped every vulnerability that was disclosed in Q1-2022 to the corresponding OWASP Top-10 and OWASP API Security Top-10 risks. This heatmap shows which of those risks prevailed.

OWASP Top-10 (2021)					OWASP API Security Top-10 (2019)
Broken Access Control	**A01**	19	4	**API1**	Broken Object Level Authorization
Cryptographic Failures	**A02**	1	3	**API2**	Broken User Authorization
Injection	**A03**	14	5	**API3**	Excessive Data Exposure
Insecure Design	**A04**	6	2	**API4**	Lack of Resources & Rate Limiting
Security Misconfiguration	**A05**	1	12	**API5**	Broken Function Level Authorization
Vulnerable and Outdated Components	**A06**	-	-	**API6**	Mass Assignment
Identification and Authentication Failures	**A07**	4	1	**API7**	Security Misconfiguration
Software and Data Integrity Failures	**A08**	1	20	**API8**	Injection
Security Logging and Monitoring Failures	**A09**	-	-	**API9**	Improper Assets Management
Server-Side Request Forgery	**A10**	2	–	**API10**	Insufficient Logging & Monitoring

Less Issues **More Issues**

Cross-Referencing OWASP Classifications

There is an open question of whether the community should have OWASP Top-10 and OWASP API Security Top-10 as two different ways of thinking about vulnerabilities. To gain some insight, we cross-mapped items from OWASP Top-10 to OWASP API Security Top-10. As you can see, the connection is not always one-to-one – it can be one-to-many.



Most Dangerous API Vulnerabilities

There are five (5) vulnerabilities with reported CVSSv3 scores greater than 9.0 – actually three of them have CVSSv3 scores of 9.8 – and one vulnerability with the CVSSv3 score of 7.5. As you can see, it's a mix of both OWASP Top-10 and OWASP API Security Top-10.

CVVSv3: **10**

CVE-2022-22947

CWE-94 Improper Control of Generation of Code ('Code Injection')

A03
OWASP API Top-10

API8
OWASP API Security Top-10

CVVSv3: **9.8**

CVE-2022-26501

CWE-863 Incorrect Authorization

A01
OWASP API Top-10

API5
OWASP API Security Top-10

CVVSv3: **9.8**

CVE-2022-23131

CWE-290 Authentication Bypass by Spoofing

A07
OWASP API Top-10

API2
OWASP API Security Top-10

CVVSv3: **7.5**

CVE-2022-24327

CWE-732 Incorrect Permission Assignment for Critical Resource

A04
OWASP API Top-10

API5
OWASP API Security Top-10

CWE-639 Authorization Bypass Through User-Controlled Key

A01
OWASP API Top-10

API1
OWASP API Security Top-10

List Of Q1-2022 API Vulnerabilities

Product	Description	CWE	OWASP Top-10 2021	OWASP Top-10 API	CVSSv3 max
Spring Cloud	CVE-2022-22947	CWE-94 Improper Control of Generation of Code ('Code Injection')	A03	API8	10
Web Server component of TIBCO Software	CVE-2022-22770	CWE-863 Incorrect Authorization, CWE-284 Improper Access Control	A01	API1	9,8
Lg TV Publix API	Lg TV Publix API auth bypass CVE-2022-23730	CWE-863 Incorrect Authorization	A01	API1	9,8
Airspan Networks Mimosa	ICS Advisory (ICSA-22-034-02) CVE-2022-21196	CWE-863 Incorrect Authorization	A01	API5	9,8
Airspan Networks Mimosa	ICS Advisory (ICSA-22-034-02) CVE-2022-21141	CWE-863 Incorrect Authorization	A01	API5	9,8
Veeam Backup & Replication	CVE-2022-26501	CWE-863 Incorrect Authorization	A01	API5	9,8
Airspan Networks Mimosa	ICS Advisory (ICSA-22-034-02) CVE-2022-21143	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	A03	API8	9,8
Pascom Cloud Phone System	Pascom: The story of 3 bugs that lead to unauthed RCE. CVE-2021-45966	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')	A03	API8	9,8
GenieACS	Validate host arg passed to ping. CVE-2021-46704	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	A03	API8	9,8
Zabbix	Zabbix Unsafe Session Storage - CVE-2022-23131	CWE-290 Authentication Bypass by Spoofing	A07	API2	9,8
Airspan Networks Mimosa	ICS Advisory (ICSA-22-034-02) CVE-2022-21215	CWE-918: Server-Side Request Forgery (SSRF)	A10	API8	9.8
Pascom Cloud Phone System	Pascom: The story of 3 bugs that lead to unauthed RCE. CVE-2021-45967	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')	A10	API8	9,8
Easy! Appointments	Exposure of Private Personal Information to an Unauthorized Actor in alextselegidis/easyappointments CVE-2022-0482	CWE-863 Incorrect Authorization	A01	API3	9.1
iRZ Mobile Routers	CVE-2022-27226: CSRF to RCE in iRZ Mobile Routers through 2022-03-16	CWE-352 Cross-Site Request Forgery (CSRF)	A01	API5	8.8

Product	Description	CWE	OWASP Top-10 2021	OWASP Top-10 API	CVSSv3 max
Veeam Backup & Replication	CVE-2022-26500	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	A01	API5	8.8
Pandora FMS API	CVE-2022-0507	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	A03	API8	8.8
Capsule Proxy	CVE-2022-23652	CWE-287 Improper Authentication	A07	API5	8.8
Grafana	Grafana 7.5.15 and 8.3.5 released with moderate severity security fixes CVE-2022-21703	CWE-352 Cross-Site Request Forgery (CSRF)	A01	A01	8.1
Pascom Cloud Phone System	Pascom: The story of 3 bugs that lead to unauthed RCE. CVE-2021-45968	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	A01	API8	7.5
Drupal	Drupal core - Moderately critical - Improper input validation - SA-CORE-2022-003 CVE-2022-25271	CWE-20 Improper Input Validation	A03	API8	7.5
Airspan Networks Mimosa	ICS Advisory (ICSA-22-034-02) CVE-2022-21176	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	A03	API8	7,5
Istio	Unauthenticated control plane denial of service attack due to stack exhaustion CVE-2022-24726	CWE-400: Uncontrolled Resource Consumption	A04	API4	7.5
JetBrains Account API	JetBrains Account exposed an API key with excessive permissions CVE-2022-24327	CWE-372 Incorrect Permission Assignment for Critical Resource	A04	API5	7.5
Istio control plane	Istio DoS vulnerability CVE-2022-23635	Improper Authentication	A07	API4	7.5
Shopware	CVE-2022-24748	CWE-287 Improper Authentication	A07	API5	7.5
Airspan Networks Mimosa	ICS Advisory (ICSA-22-034-02) CVE-2022-0138	CWE-502: Deserialization of Untrusted Data	A08	API8	7,5
Liferay API	Liferay API auth bypass CVE-2021-38268	CWE-276 Incorrect Default Permissions	A01	API5	6,5
pimcore	Pimcore API is vulnerable to Path Traversal attacks CVE-2022-0665	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	A01	API8	6.5
Cisco SD-WAN vManage Software	Cisco SD-WAN vManage Software Information Disclosure Vulnerability CVE-2022-20747	CWE-202: Exposure of Sensitive Information Through Data Queries	A01	-	6.5

Product	Description	CWE	OWASP Top-10 2021	OWASP Top-10 API	CVSSv3 max
Airspan Networks Mimosa	ICS Advisory (ICSA-22-034-02) CVE-2022-21800	CWE-327: Use of a Broken or Risky Cryptographic Algorithm	A02	API2	6.5
ePolicy Orchestrator (ePO)	Security Bulletin - ePolicy Orchestrator update addresses multiple product vulnerabilities (CVE-2022-0842, CVE-2022-0857, CVE-2022-0858, CVE-2022-0859, CVE-2022-0861, CVE-2022-0862) and updates Java, Apache HTTP Server, and Tomcat CVE-2022-0859	CWE-522: Insufficiently Protected Credentials	A04	API3	6,5
Aruba switches	Aruba switches CVE-2021-41003	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	A03	API8	6.1
Swagger	Add an enableQueryConfig option CVE-2021-46708	CWE-1021 Improper Restriction of Rendered UI Layers or Frames	A04	API7	6.1
Xwiki API	Xwiki API-based Auth Bypass (partial) CVE-2022-23615	CWE-863 Incorrect Authorization	A01	API5	5.4
Grafana	Grafana 7.5.15 and 8.3.5 released with moderate severity security fixes CVE-2022-21702	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	A03	API8	5.4
ePolicy Orchestrator (ePO)	Security Bulletin - ePolicy Orchestrator update addresses multiple product vulnerabilities (CVE-2022-0842, CVE-2022-0857, CVE-2022-0858, CVE-2022-0859, CVE-2022-0861, CVE-2022-0862) and updates Java, Apache HTTP Server, and Tomcat	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	A03	API8	5.4
ePolicy Orchestrator (ePO)	Security Bulletin - ePolicy Orchestrator update addresses multiple product vulnerabilities (CVE-2022-0842, CVE-2022-0857, CVE-2022-0858, CVE-2022-0859, CVE-2022-0861, CVE-2022-0862) and updates Java, Apache HTTP Server, and Tomcat	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	A03	API8	4.3
Grafana	Grafana 7.5.15 and 8.3.5 released with moderate severity security fixes CVE-2022-21713	CWE-863 Incorrect Authorization	A01	API5	4.3

Product	Description	CWE	OWASP Top-10 2021	OWASP Top-10 API	CVSSv3 max
ePolicy Orchestrator (ePO)	Security Bulletin - ePolicy Orchestrator update addresses multiple product vulnerabilities (CVE-2022-0842, CVE-2022-0857, CVE-2022-0858, CVE-2022-0859, CVE-2022-0861, CVE-2022-0862) and updates Java, Apache HTTP Server, and Tomcat	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	A03	API8	4.3
ePolicy Orchestrator (ePO)	Security Bulletin - ePolicy Orchestrator update addresses multiple product vulnerabilities (CVE-2022-0842, CVE-2022-0857, CVE-2022-0858, CVE-2022-0859, CVE-2022-0861, CVE-2022-0862) and updates Java, Apache HTTP Server, and Tomcat	CWE-611: Improper Restriction of XML External Entity Reference	A05	API8	3.5
ePolicy Orchestrator (ePO)	Security Bulletin - ePolicy Orchestrator update addresses multiple product vulnerabilities (CVE-2022-0842, CVE-2022-0857, CVE-2022-0858, CVE-2022-0859, CVE-2022-0861, CVE-2022-0862) and updates Java, Apache HTTP Server, and Tomcat	CWE-522: Insufficiently Protected Credentials	A04	API3	3.1
Gradle	Default installation configuration allows anonymous access to some admin configuration	CWE-276 Incorrect Default Permissions	A01	API1	*
Microsoft Azure	Insecure Direct Object Reference (IDOR) Exposes all users of Microsoft Azure Independent Software Vendors	CWE-639: Authorization Bypass Through User-Controlled Key	A01	API1	*
FTS Web UI	API and Websocket Keys Leakage	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	A01	API3	*
Statamic CMS	Prevent filtering users by password hashes in the APIs	CWE-20 Improper Input Validation	A04	API3	*
Shopify	Orders full read for a staff with only `Customers` permissions.	CWE-285: Improper Authorization	A01	API5	*
Cipi Control Panel	Cipi Control Panel 3.1.15 - Stored Cross-Site Scripting (XSS) (Authenticated)	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	A03	API8	*
ungit	Potential remote code exec	CWE-94: Improper Control of Generation of Code ('Code Injection')	A03	API8	*

About Wallarm

Wallarm end-to-end API security products provide robust protection for APIs, microservices, and serverless workloads running in cloud-native environments. Hundreds of Security and DevOps teams chose Wallarm to get unique visibility into malicious traffic, robust protection across the whole API portfolio, and automated incident response for product security programs.

The company is committed to supporting modern tech stacks, offering dozens of deployment options in cloud and Kubernetes-based environments, and also provides a full cloud solution. Wallarm is headquartered in San Francisco, California, and is backed by Toba Capital, Y Combinator, Partech, and other investors.

Join API Security LinkedIn community
https://www.linkedin.com/groups/12624726/

Book a Wallarm demo
or start your free trial now

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