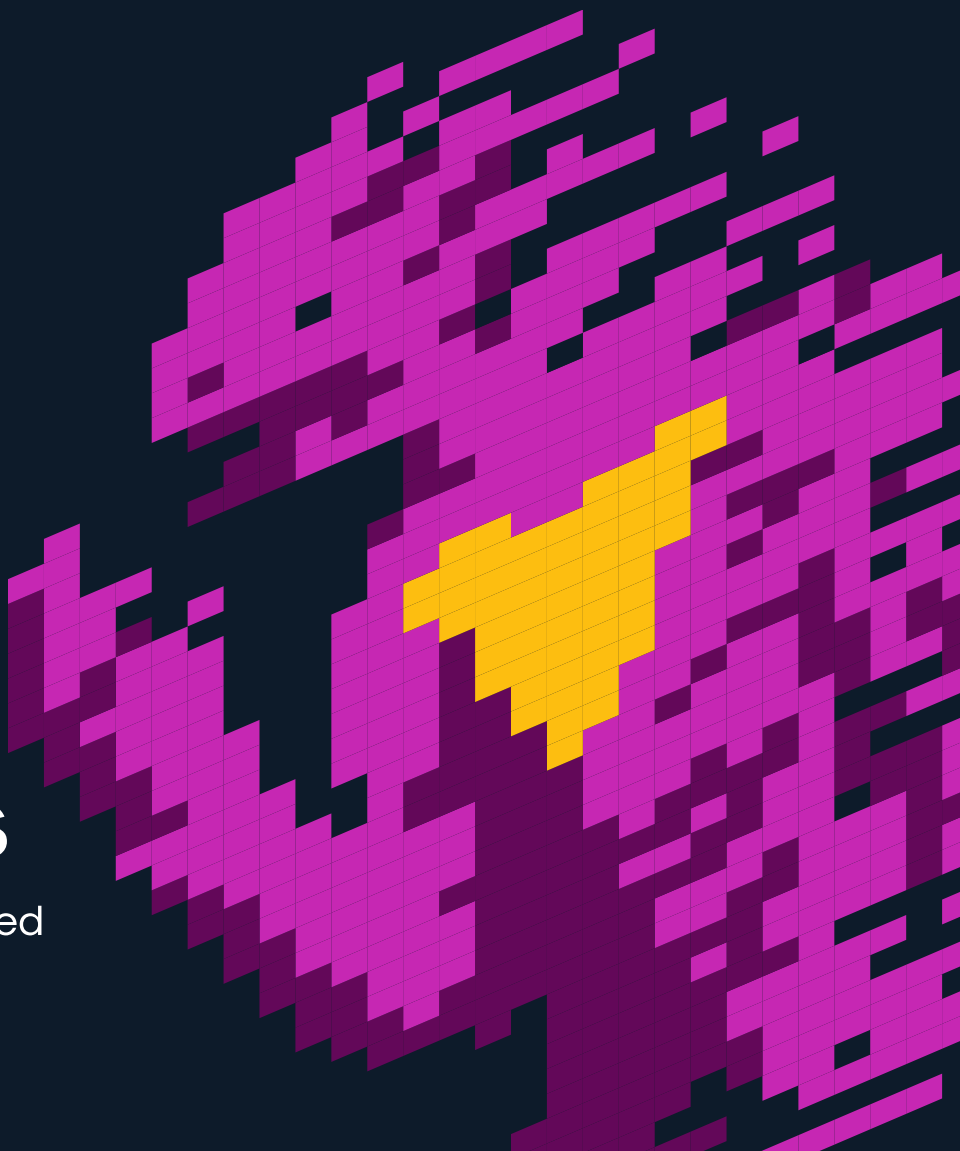
wallarm

RESEARCH REPORT

API ThreatStats™ Report Q2-2023

Top API Vulnerabilities & Exploits

The Oldest, the Most Sophisticated, the Most Impactful, the Most Viral API Exploits of Q2-2023 that you need to know about.



63%

of bug bounty rewards in H1-2023 related to APIs

See page 4 →

39 months

Oldest API exploit discovered in Q2-2023

See page 7 →

Introduction

Welcome to the latest **Wallarm API ThreatStats report**, which provides API builders, defenders and breakers a comprehensive look at the API security vulnerabilities, threats, and exploits reported in Q2-2023.

Long-time readers will notice that we've changed our reporting:

- **Follow the Money.** We are expanding our coverage to include, for the first time, analysis of bug bounty rewards.
- **API Security Razzies.** We're reducing our statistical coverage and homing in on the most impactful vulnerabilities and exploits of the quarter.

API-Related Bug Bounties

We continue to see a steady increase in API vulnerabilities and exploits this year. An amazing 63% of all HackerOne bug bounty rewards paid so far this year were for API security problems, with a total of $26,490 being paid out in just the last quarter. As bounty payments typically lag by 2-3 months, we anticipate an even greater surge in these payments for vulnerabilities reported in Q2.

63%

of all bug bounty rewards paid so far in 2023 are for API vulnerabilities

39 months

the oldest API zero-day exploit found in Q2-2023

Our First API Security Razzies

As always, we've analyzed all published CVEs, security bulletins, and bug bounty reports to bring you the most insightful perspectives on API security. From this analysis, we are selecting the most impactful results for Q2-2023 in the following categories:

- Top Bug Bounty Rewards
- Oldest Exploit
- Most Viral Exploit
- Most Dangerous Exploit
- Most Sophisticated Exploit
- Top AI-related Exploit
- Top Enterprise Exploit

Reading this report, you'll quickly realize that API exploits are pervasive across a range of sectors, from AI hardware to enterprise infrastructures, DevOps tools, and even major cloud providers' management software. They are everywhere because APIs are everywhere, and their ubiquity only amplifies their potential risk. The danger they pose is significant, primarily because APIs serve as direct gateways to data.

Read on, for knowledge is the first line of defence.

Best regards,
Wallarm API Security Research Team

API Threat Landscape

32.1M
unique API attacks
[40% of all Q2-2023 attacks]

OWASP APIsec Top-10

47.5M
unique non-API attacks
[60% of all Q2-2023 attacks]

OWASP Top 10

+60%
rise in unique API attacks QoQ
(Q2-2023 vs. Q1-2023)

+514%
rise in detected API attacks YoY
(Q2-2023 vs. Q2-2022)

The unique ability of Wallarm to detect both API-specific and non-API attacks allows us to highlight API attack trends within all web attacks. In Q2-2023 we saw a 40/60 split between OWASP APIsec Top-10 and OWASP Top-10 across all web attacks. Interestingly, this correlates with API / non-API bug bounty rewards paid over this quarter (see page 4).

We project that next quarter we will see API attacks exceed the number of non-API web attacks for the first time ever.

40% of all web attacks were API-related in Q2-2023, compared to **18%** in Q2-2022

6x malicious requests per API attack sequence YoY

The average number of malicious requests per API attack sequence increased to 30 in Q2-2023 from 22 in Q1-2023, up from 5 requests per attack in Q2-2022. This is another indicator that APIs attacks are increasingly more consistent and sophisticated.

Top Bug Bounty Rewards

We mined bug bounty data from HackerOne to understand where breakers are putting their efforts. It turns out that a significant number of bug bounty payouts over the last two quarters are API-related.

44% / 63%

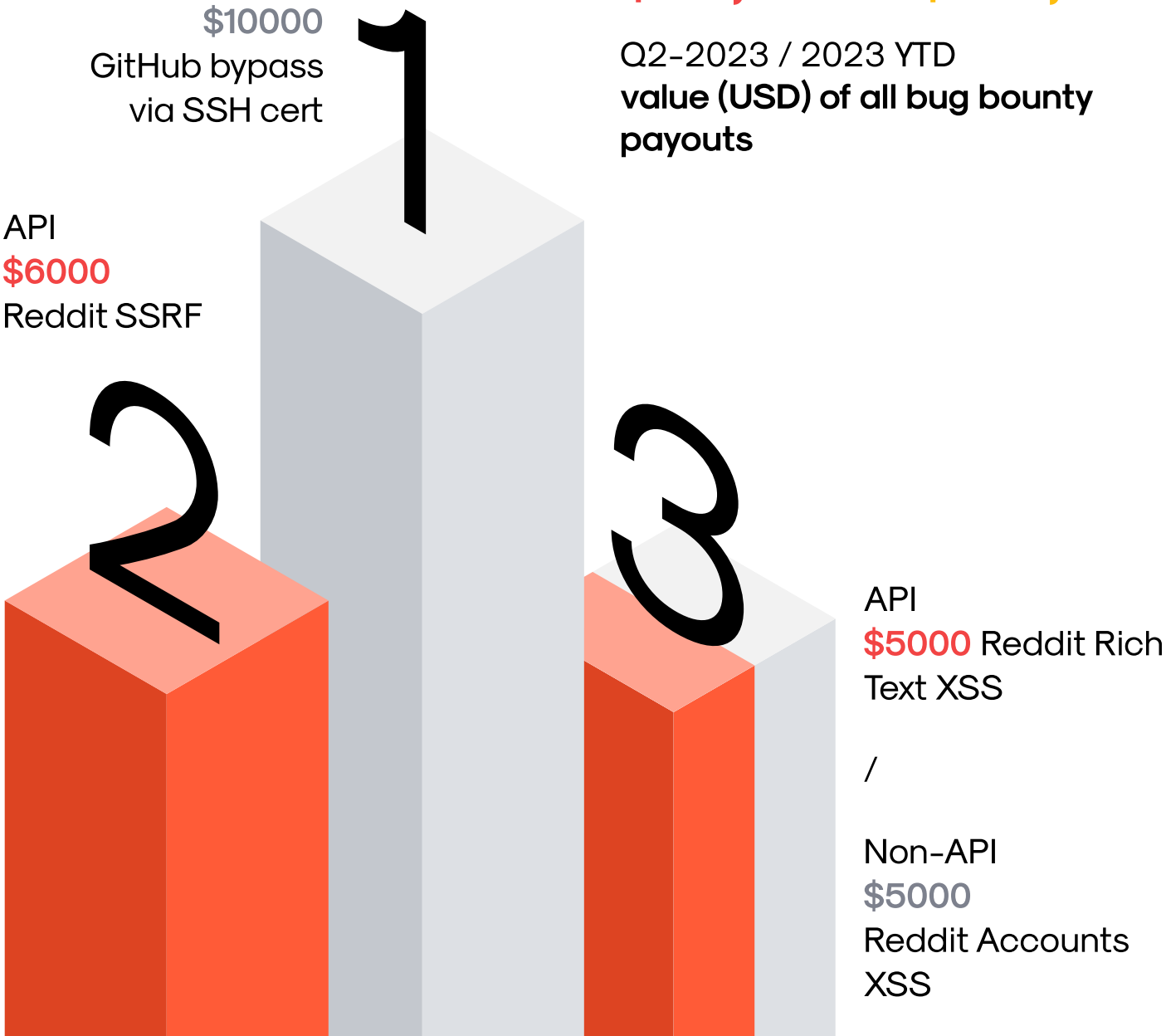
Q2-2023 / 2023 YTD
pct of API bug bounties vs. all payouts

$26,490 / $121,150

Q2-2023 / 2023 YTD
value (USD) of API bug bounty payouts

$59,720 / $193,110

Q2-2023 / 2023 YTD
value (USD) of all bug bounty payouts



Biggest API Bug Bounty of Q2-2023

$6000 for Reddit SSRF, and the 2nd biggest payment of Q2'23

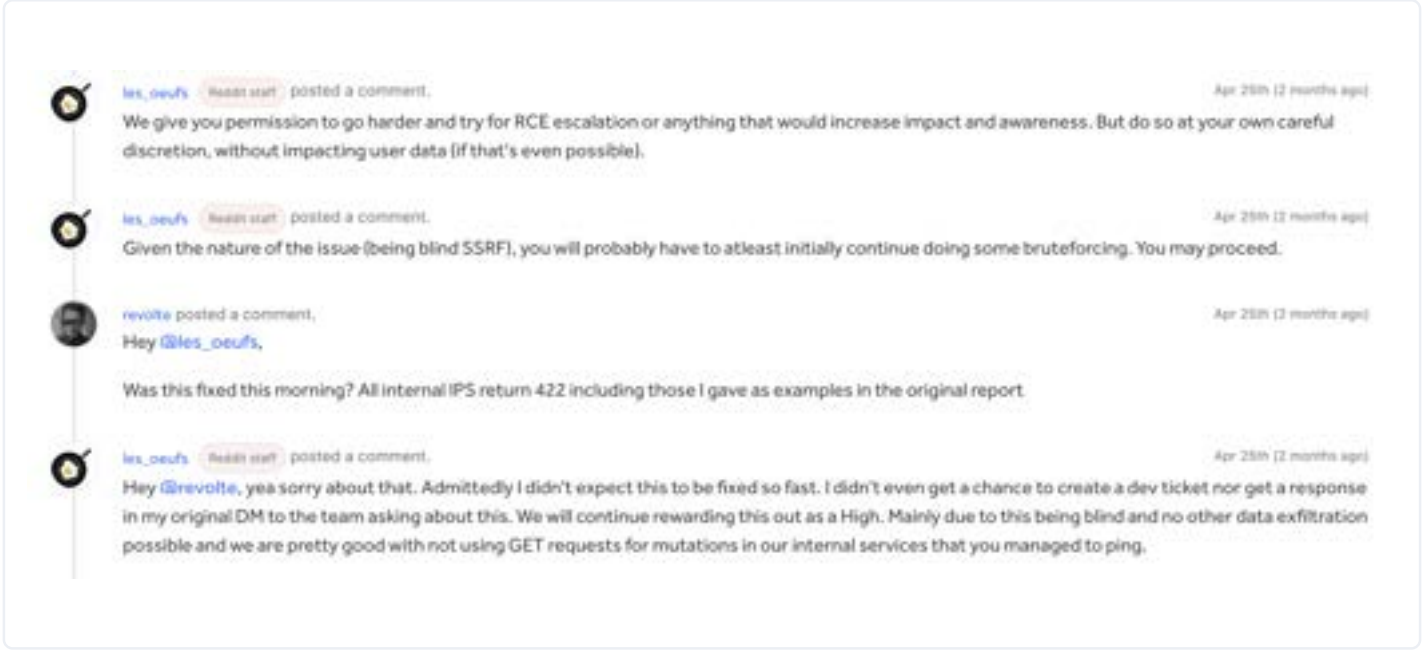
Matrix Chat endpoint at

```
https:/matrix.redditspace.com/
_matrix/media/r0/preview_url/?url=*
```

allowed partially blind SSRF to internal services. The data that could be exfiltrated was limited only to the service names and their IPs before a fix was implemented.

This endpoint should not be able to query internal services, but external IPs, domains, and services are fine for this to query.

Bug hunter @revolte was attempting to escalate this SSRF to RCE but Reddit fixed it before it happened.



Reference: https://hackerone.com/reports/1960765

API Time-to-Exploit in Q2-2023

– 19 days

Average API time-to-exploit in Q2-2023

– 1182 days

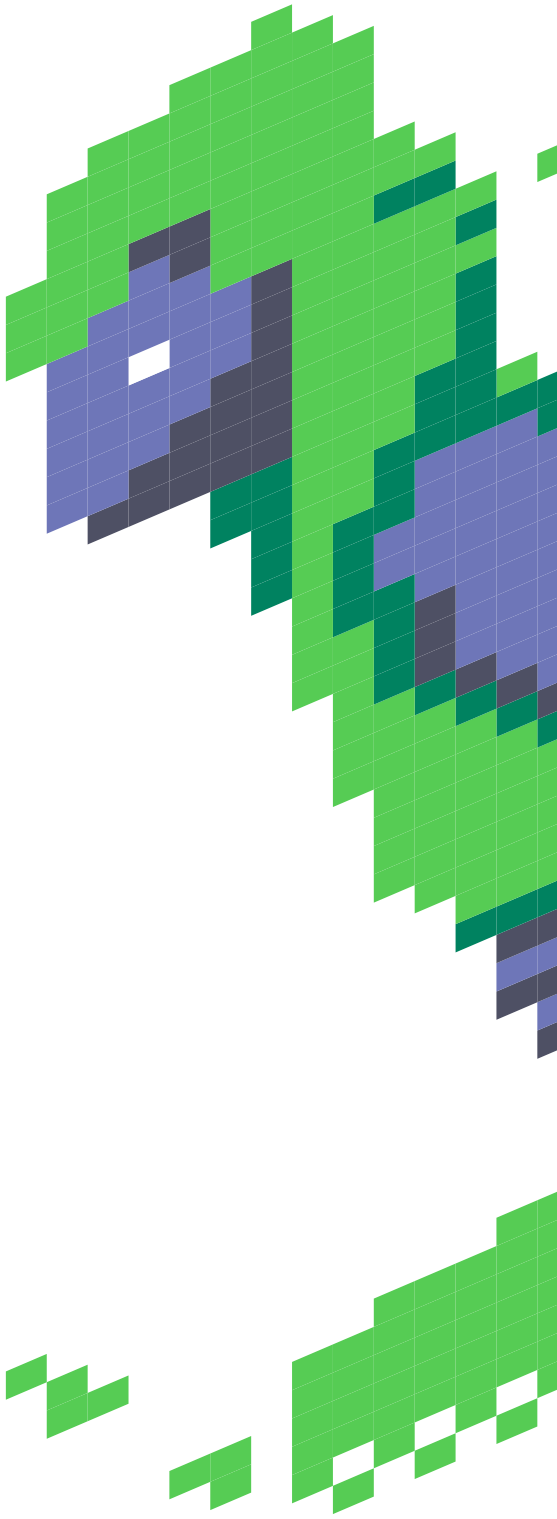
Longest pre-CVE time-to-exploit
interval in Q2-2023
WordPress MStore API plugin

+164 days

Longest post-CVE time-to-exploit
interval in Q2-2023
Livebox Collaboration vDesk

40%

Pct of API 0-day vs. post-CVE exploits
found in Q2-2023



Oldest API Exploit in Q2-2023

CVSS 9.8

1132 days (over 39 months!)
elapsed between exploit POC and CVE being published

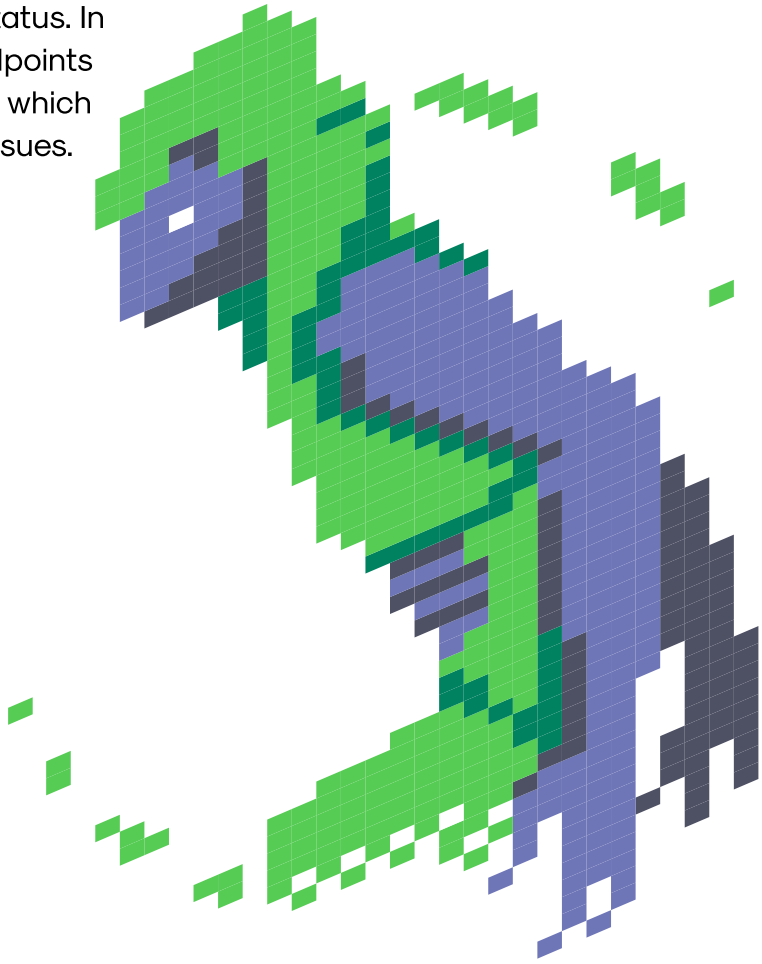
An Authentication Bypass vulnerability was discovered in certain versions of the MStore API plugin for WordPress which could allow unauthenticated users to create or edit administrator accounts. First reported publicly in Mar-2020, this vulnerability was finally published as CVE-2020-36713 in Jun-2023.

The plugin registers several custom endpoints in the

```
"mstore-api/controllers/FlutterUser.php"
```

script via the WP REST API. Among these are the **register** and **update_user_profile** routes, which are accessible to any user regardless of authentication status. In addition, the MStore API registers several custom endpoints via the WP JSON API plugin, deprecated in Aug-2019, which should not be activated because of critical security issues.

Although this vulnerability was responsibly reported and patched in Feb-2020, vulnerability management programs which rely solely on published CVEs would have been exposed for over 3 years. This points to the need for a multi-faceted security approach including automating updates, scouring vendor reports, and implementing solid NG-WAF protection.



Most Viral API Exploit

MOVEit Transfer SQL Injection Vulnerabilities

CVE-2023-34362 (CVSS score: 9.8)
CVE-2023-35036 (CVSS score: 9.1)
CVE-2023-35708 (CVSS score: 9.8)

Several serious security vulnerabilities in the MOVEit Transfer application were identified in Q2-2023. These are SQL injections in some of the API calls that can lead to remote code execution (RCE). This exploit attack surface is still expanding, with additional vulnerabilities being found as we move into Q3.

The cl0p ransomware gang exploited these vulnerabilities in the MOVEit file transfer tool, potentially dating back as far as 2021, leading to the compromise of personal data for more than 15.5 million individuals across various organizations globally, including government bodies, educational institutions, finance, and insurance companies, to name a few. With many victims still undisclosed and the attacks continuing, the final count of affected individuals and organizations remains unknown.

13M

pages of coverage in Q2 on the MOVEit vulnerabilities

0.5%

of all API Security content in Q2 mentioned the MOVEit vulnerabilities

Reference: https://lab.wallarm.com/the-moveit-ransomware-attacks-now-impacting-government-agencies-and-large-organizations/

Most Dangerous API Exploit of Q2-2023

CVSS 9.8

This ESPv2 vulnerability (CVE-2023-30845) impacting the Google Cloud Platform (GCP) should serve as an important reminder to update your cybersecurity policies and risk management strategies to include open-source API infrastructure tools. This L7 service proxy for managing JSON/REST and gRPC API services was exposed to an authentication bypass vulnerability that had serious potential security implications.

The loophole enabled API clients to create a malicious X-HTTP-Method-Override header value, thereby circumventing JWT authentication under certain conditions. Unauthorized actors could potentially gain access to restricted data or services if the HTTP method requested was not present in the API service definition and if the given X-HTTP-Method-Override was a valid HTTP method according to the service definition:

```
curl --request PUT  \
     --header "X-HTTP-Method-Override: POST" \
     --header "Content-Type: application/json" \
     --data '{"payload":"compromised"}' \
     https://url-to-espv2.com
```

The malicious client successfully bypasses Using Google ID tokens to authenticate users without specifying a JWT:

```
{"message":"Accessing restricted
method.","method":"POST","payload":"compro
mised"}
```

Reference: https://lab.wallarm.com/gcp-espv2-hit-with-critical-api-authorization-bypass-cve-2023-30845/

Most Sophisticated API Exploit in Q2-2023

CVSS 7.5

Grafana JWT URL-login flow leaks access tokens.

Grafana is a widely adopted open-source DevOps platform for monitoring and observability. An issue (CVE-2023-1387) reported in Q2-2023 concerns leakage of an auth token in the JWT URL-login flow. The problem occurs when Grafana proxies requests without removing the auth_token parameter, leading to potential unauthorized access to Grafana as the victim user.

This exploit, which is quite complicated but very interesting and unique, suggests what sophisticated attacks against your APIs might look like.

1. First, an instance of Grafana with JWT authentication enabled is set up. This can be done using a Docker container with the necessary environment variables set to enable JWT authentication and URL login.
2. The user then configures a Prometheus data source, setting the URL to a server where intercepted requests can be viewed.
3. A JWT token is obtained from the Auth0 instance using a curl request with the client ID, client secret, subdomain, username, and password.
4. The obtained id_token is used to make a request to the Grafana instance.
5. Grafana authenticates the user and forwards the request to the data source, but leaves the JWT in place.
6. The catch server receives the request containing the JWT in the request parameters.

In comparison, if the JWT is passed in the header (X-JWT-Assertion), the auth header is removed from the proxy request, and no leakage occurs.

Reference: https://github.com/grafana/bugbounty/security/advisories/GHSA-5585-m9r5-p86j

Top AI-related API Exploit of Q2-2023

CVSS 8.8

NVIDIA DGX-1 BMC Arbitrary Command Injection in SPX REST API

A critical API vulnerability, labelled CVE-2023-25507, was discovered in the NVIDIA DGX-1 AI supercomputer system. This vulnerability lies in the DGX-1's Baseboard Management Controller (BMC) SPX REST API, enabling an authorized attacker to inject arbitrary shell commands. Exploitation of this vulnerability could lead to malicious code execution, denial of service, information disclosure, and data tampering.

AI systems like the DGX-1 handle significant amounts of sensitive data, making security crucial. A successful attacker could manipulate AI models by altering data, which could lead to inaccurate results and would be very difficult to root cause. They could also leak sensitive information, disrupt services, or gain control over the system.

This vulnerability emphasizes the importance of robust API security measures in AI applications. To mitigate such risks, it's essential to implement regular updates & strong access controls, and conduct penetration testing. NVIDIA has released patches to fix this vulnerability and users are urged to update their systems promptly. As use of AI systems grow, so does the importance of maintaining robust security practices, especially around APIs.

Reference: https://nvidia.custhelp.com/app/answers/detail/a_id/5458

Top Enterprise API Exploit of Q2-2023

CVSS 8.8

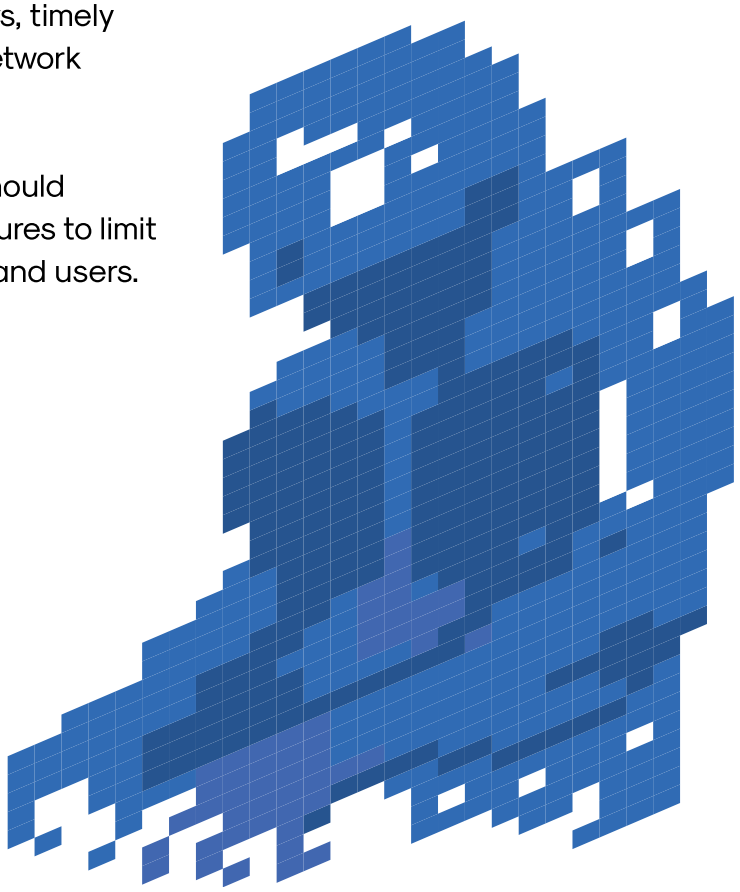
Juniper JunOS gRPC Arbitrary Command Injection

A significant OS Command Injection vulnerability has been identified in the gRPC Network Operations Interface (gNOI) server module of Junos OS Evolved, a key component of Juniper Network security devices often incorporated in enterprise networks. This vulnerability (CVE-2023-28983) could allow authenticated, low-privileged, network-based attackers to inject shell commands and execute code.

In the context of enterprise networks, where Juniper devices are a common presence, this vulnerability underscores the paramount importance of API security.

Juniper Networks has addressed this High severity issue with updates in version 22.2R1-EVO and later. As always, timely firmware updates are vital in maintaining robust network protection.

To further mitigate exploitation risks, companies should implement and periodically review & update measures to limit access to trusted administrative networks, hosts, and users.



About Wallarm

At Wallarm, we understand the unique challenges and threats that come with the ever-evolving digital landscape. That's why we're committed to developing cutting-edge API security solutions that enable businesses to secure their digital assets effectively. As your trusted partner, we not only protect your business but also empower it to thrive in the digital economy.

API Discovery Controls

We ensure full visibility and management of your API portfolio through automatic endpoint discovery, schema building based on actual traffic, and tracking of API changes.

API Leak Management

Wallarm scans for, blocks, and controls the use of leaked API secrets to protect your data and infrastructure.

Sensitive API Data Classification

Wallarm classifies API endpoints by Personally Identifiable Information (PII), tracks sensitive data in API endpoints, and prevents the use of leaked API keys.

API Threat Prevention

Wallarm offers comprehensive security for APIs and legacy web apps covering all OWASP Top-10 risks, proactive attack prevention, protection against malicious automated tools, and an ML-based automated tuning approach with smart blocking from day 1.

Wallarm is a global leader in API security, headquartered in San Francisco. We proudly serve a broad spectrum of clients, including Fortune 500 companies and hypergrowth SaaS startups across numerous industries such as finance, healthcare, and technology.

Follow us on LinkedIn to stay in touch with the latest API security threats discoveries and risk analysis.

www.linkedin.com/company/wallarm

Wallarm Research Team
lab.wallarm.com

wallarm

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