

CVE-2022-24112

Apache APISIX Authentication Bypass Vulnerability

Exigent

CISA KEV since Aug 25, 2022

Actively exploited

Public exploit module (Metasploit)

An attacker can abuse the batch-requests plugin to send requests to bypass the IP restriction of Admin API. A default configuration of Apache APISIX (with default API key) is vulnerable to remote code execution. When the admin key was changed or the port of Admin API was changed to a port different from the data panel, the impact is lower. But there is still a risk to bypass the IP restriction of Apache APISIX's data panel. There is a check in the batch-requests plugin which overrides the client IP with its real remote IP. But due to a bug in the code, this check can be bypassed.

EVRS 86/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.961 99.88th percentile · FIRST	CISA DEADLINE Sep 15, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.961 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
apisix	< 2.10.4 ≥ 2.11.0 < 2.12.1	2.10.4 · 2.12.1	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-2vc7-6w39-6rh2	Additional guidance	lists.apache.org/thread/lcdqywz8zy94mdysk7p3gfdgn51jmt94
NVD	nvd.nist.gov/vuln/detail/CVE-2022-24112	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-29024	Current data	evulnabile.com/vulnerability-management/cve/CVE-2022-24112

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.