CVE-2022-24112 - Score: 9.8

Components:

apache apisix *

Description:

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.

Main problems:

290 "Authentication Bypass by Spoofing"