


New issue

Jump to bottom

Requests that follow a redirect are not passing via the proxy #3369

 Closed aSapien opened this issue on Oct 29, 2020 · 14 comments · Fixed by #3410

Projects  v0.21.1
Milestone  v0.21.1

aSapien commented on Oct 29, 2020 • edited

Describe the bug

In cases where `axios` is used by servers to perform http requests to user-supplied urls, a proxy is commonly used to protect internal networks from unauthorized access and [SSRF](#). This bug enables an attacker to bypass the proxy by providing a url that responds with a redirect to a restricted host/ip.

To Reproduce

The following code spawns a proxy server that *always* responds with a 302 redirect, so requests should never reach the target url, however, `axios` is only reaching the proxy once, and bypassing the proxy after the redirect response.

<https://runkit.com/embed/1df5qy8lbgnc>

```
const axios = require('axios')
const http = require('http')

const PROXY_PORT = 8080

// A fake proxy server
http.createServer(function (req, res) {
  res.writeHead(302, {location: 'http://example.com'})
  res.end()
}).listen(PROXY_PORT)

axios({
  method: "get",
  url: "http://www.google.com/",
  proxy: {
    host: "localhost",
    port: PROXY_PORT,
  },
}).then((r) => console.log(r.data))
.catch(console.error)
```

The response is the rendered html of <http://example.com>

Expected behavior

All the requests should pass via the proxy. In the provided scenario, there should be a redirect loop.

Environment

- Axios Version [0.21.0]
- Node.js Version [v12.18.2]

Additional context/Screenshots

Add any other context about the problem here. If applicable, add screenshots to help explain.

 32

 aSapien added the `status:possible bug` label on Oct 29, 2020

marikaner commented on Oct 30, 2020

I am not 100% sure yet, but I think we are encountering the same issue. I get an `getaddrinfo ENOTFOUND` error and I think this is due to the fact that the proxy agent is missing in the redirected request. (I will investigate more, though).

chinesedfan commented on Nov 1, 2020

Collaborator

@RubenVerborgh Maybe axios should set `beforeRedirect` of follow-redirects?

RubenVerborgh commented on Nov 1, 2020

Yes, that seems to be the case.

marikaner commented on Nov 3, 2020

Does anyone have an idea for a workaround?

This was referenced on Nov 4, 2020

Batch Csrf token error SAP/cloud-sdk-js#617

Closed

fix: Workaround csrf redirects SAP/cloud-sdk-js#667

Merged

marikaner commented on Nov 4, 2020

I found that this is in fact the cause of our issues. I fixed it for us with a workaround, but an actual fix would be much appreciated.

The workaround is, that in case of an error I set the url of the redirected request in the old config and execute the request again:

```
axios.request(myConfig).catch(error => {  
  if (error.request._isRedirect) {  
    return axios.request({  
      ...myConfig,  
      url: error.request._options.path  
    });  
  }  
});
```

christian-kreuzbe... commented on Nov 10, 2020

Thanks for the workaround!

Just to wrap this up: if we're not using the `proxy` feature of axios, we should not be affected by this?

2

marikaner commented on Nov 11, 2020

Yes, that is my understanding. Only the combination of proxy + redirects.

timemachine3030 mentioned this issue on Nov 12, 2020

Hotfix: Prevent SSRF #3410

Merged

carnil commented on Nov 13, 2020

[CVE-2020-28168](#) appears to have been assigned to this issue.

timemachine3030 commented on Nov 15, 2020

Contributor

Anyone listening on this issue, Code review of [#3410](#) is needed.

5

KrayzeeKev commented on Nov 22, 2020

SourceClear have rated this CVE a 7.5 which means that all our pipelines are failing to build. It'd be really good if [#3410](#) could be merged as we can no longer deploy our software without raising all manner of engagements with corporate security.

jasonsaayman added this to the **v0.21.1** milestone on Nov 23, 2020

jasonsaayman closed this as completed in [#3410](#) on Nov 24, 2020

jasonsaayman commented on Nov 24, 2020

Member

Please see [#3410](#) this will be released in 0.21.1

mdeknewis commented on Dec 3, 2020

Hallo, is there any schedule to release 0.21.1, so the vulnerability is fixed and all dependent projects can fix their vulnerabilities?

39

kerimkaan mentioned this issue on Dec 13, 2020

CVE-2020-28168 - Medium Severity Vulnerability Unitech/pm2#4937

Open

snoopfab mentioned this issue on Dec 18, 2020

Server-Side Request Forgery (SSRF) Affecting one of your dependency : axios package, ALL versions jgoralcz/aki-api#76

Closed

 corydorning mentioned this issue on Jan 4, 2021

Ditch @serverless/platform-sdk in favor of @serverless/platform-client serverless/dashboard-plugin#464

Closed

 christiang mentioned this issue on Jan 4, 2021

Upgrade to axios 0.21.1 to address outstanding security alert microsoft/FluidFramework#4709

Closed

 sysdotini mentioned this issue on Jan 5, 2021

deps: bump axios (npm advisory #1594) MenuDocs/erela.js-spotify#5

Merged

 snuggs mentioned this issue on Jan 5, 2021

Browser Sync vulnerability ... (again) devpunks/snuggsi#215

Open

 phin3has mentioned this issue on Jan 6, 2021

Need to upgrade Axios Coalfire-Research/npk#136

Closed

 dhartunian mentioned this issue on Jan 11, 2021

[Snyk] Security upgrade analytics-node from 3.4.0-beta.1 to 3.5.0 cockroachdb/cockroach#58484

Closed

 alphaolomi mentioned this issue on Jan 13, 2021

chore: bump axios to "^0.21.1" AfricasTalkingLtd/africastalking-node.js#87

Closed

 DanielNetzeriAm mentioned this issue on Jan 24, 2021

Axios version have security issues waldophotos/kafka-avro#102

Closed

 dnotes mentioned this issue on Jan 26, 2021

Update axios to 0.21.1 jovotech/jovo-framework#887

Closed

4 tasks

mikesir87 commented on Jan 28, 2021

Just as an FYI in case someone comes across this via a Google Search... incognito Chrome windows currently block third-party cookies, which will cause this error. So, either disable the feature (Settings -> Cookies and other site data -> Block third-party cookies in Incognito) or drop out of incognito.

 codyborn mentioned this issue on Feb 24, 2021

Upgrade dependencies of axios celo-org/celo-monorepo#7269

Merged

 mergify (bot) pushed a commit to celo-org/celo-monorepo that referenced this issue on Feb 25, 2021

 Upgrade dependencies of axios (#7269) ...

4699f8d

 FrankEssenberger mentioned this issue on Feb 26, 2021

CSRF token validation failed - SAP Business Application Studio destination with on-premise destination SAP/cloud-sdk-js#1037

Closed

 rohan-deshpande mentioned this issue on Mar 25, 2021

high severity vulnerability RealFaviconGenerator/cli-real-favicon#18

Open

 **aszx87410** mentioned this issue on Mar 28, 2021

VolgaCTF 2021 Qualifier - Unicorn Networks aszx87410/ctf-writeups#29

 Open

 **kitloong** mentioned this issue on Apr 1, 2021

Bump axios from 0.19.0 to 0.21.1 rakutentech/node-alertnotification#8

 Closed

 This was referenced on Apr 27, 2021

Current delivery SDK release has high priority vulnerability with Axios amplience/dc-delivery-sdk-js#43

 Closed

Current management SDK release has high priority vulnerability with Axios amplience/dc-management-sdk-js#85

 Closed

 **github-actions**  mentioned this issue on Jun 6, 2021

Vulnerability Himavanth/hima#10

 Closed

 **debricked**  mentioned this issue on Jul 1, 2021

Bulk vulnerability fix - Lockfile fix depricked/a-wild-button-appears#1

 Open

SergeyKoval commented on Aug 17, 2021

Looks like in 0.21.1 it is still actual...

 1

 **badluboy** mentioned this issue on Mar 20

<!-- Click "Preview" for a more readable version --> badluboy/github-slideshow#2

 Open

 This was referenced on May 10

Using config.beforeRedirect prevents using proxy on redirected requests #4703

 Closed

Fixing proxy beforeRedirect regression #4708

 Merged

 **Abdul1110** mentioned this issue on May 11

CVE-2020-28168 @ Npm-axios-0.19.0 Abdul1110/TEST_ORION#39

 Open

Assignees

No one assigned

Labels

None yet

Projects

No open projects


1 closed project ▾

Milestone

v0.21.1

Development

Successfully merging a pull request may close this issue.

 **Hotfix: Prevent SSRF**
timemachine3030/axios

12 participants

