

[New issue](#)[Jump to bottom](#)

authorization header is not deleted on redirects to third party origins #872

✓ Closedszmarczak opened this issue on Jul 11, 2021 · 0 comments · Fixed by [#875](#)

Labels

bug

szmarczak commented on Jul 11, 2021

Member

Bug Description

Security flaw.

Reproducible By

```
const http = require('http');
const undici = require('undici');

const server = http.createServer((request, response) => {
  if (request.headers.authorization !== 'test') {
    response.statusCode = 403;
    response.end();
    return;
  }

  response.statusCode = 302;
  response.setHeader('location', 'https://httpbin.org/anything');
  response.end();
});

server.listen(8080, async () => {
  const {statusCode, headers, body} = await undici.request('http://localhost:8080', {
    maxRedirects: 3,
    headers: {
      authorization: 'test'
    }
  });
});
```

```
const chunks = [];  
for await (const chunk of body) {  
  chunks.push(chunk);  
}  
  
const parsed = JSON.parse(Buffer.concat(chunks));  
console.log(parsed.headers.Authorization);  
  
undici.getGlobalDispatcher().destroy();  
server.close();  
});
```

Expected Behavior

The `authorization` header should be deleted when redirecting to third party origin.

Environment

Linux solus 5.13.1-187.current #1 SMP PREEMPT Wed Jul 7 19:52:26 UTC 2021 x86_64 GNU/Linux
Node v16.4.2
undici@4.1.0

  **szmarczak** added the `bug` label on Jul 11, 2021

  **szmarczak** mentioned this issue on Jul 11, 2021

fix: remove `authorization` header when redirecting to unknown origins #875

 Merged

 **mcollina** closed this as completed in [#875](#) on Jul 12, 2021

Assignees

No one assigned

Labels

bug

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **fix: remove `authorization` header when redirecting to unknown origins**
szmarczak/undici

1 participant

