CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting)

Moderate **jknack** published **GHSA-gv3v-92v6-m48j** on Apr 2, 2020 · 1 comment

Package

io.jooby:jooby-netty (Java, Maven, Gradle)

Affected versions	Patched versions
< 2.2.1	2.2.1

Description

Impact

- Cross Site Scripting
- Cache Poisoning
- Page Hijacking

Patches

This was fixed in version `2.2.1`.

Workarounds

If you are unable to update, ensure that user supplied data isn't able to flow to HTTP headers. If it does, pre-sanitize for CRLF characters.

References

CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')

I've been poking at libraries to see if they are vulnerable to HTTP Response Splitting and Jooby is my third case of finding this vulnerability.

Root Cause

This roots cause back to this line in the Jooby codebase:

jooby/modules/jooby-netty/src/main/java/io/jooby/internal/netty/NettyContext.java
Line 102 in `93cfc80`

```
102     final DefaultHttpHeaders setHeaders = new DefaultHttpHeaders(false);
```

The `DefaultHttpHeaders` takes a parameter `validate` which, when `true` (as it is for the no-arg constructor) validates that the header isn't being abused to do HTTP Response Splitting.

Reported By

This vulnerability was reported by **@JLLeitschuh** (Twitter)

For more information

If you have any questions or comments about this advisory:

- Open an issue in jooby-project/jooby

Severity

Moderate

CVE ID

CVE-2020-7622

Weaknesses

No CWEs

Credits


JLLeitschuh