CRLF injection in request path, method, and headers

Moderate **mcollina** published **GHSA-3cvr-822r-rqcc** on Jul 18

Package

undici (npm)

Affected versions	Patched versions
< v5.7.1	>= v5.8.0

Description

Impact

It is possible to inject CRLF sequences into request headers in Undici.

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

const response = undici.request("http://127.0.0.1:1000", {
  headers: {'a': "\r\nb"}
})
```

The same applies to `path` and `method`

Patches

Update to v5.7.1

Workarounds

Sanitize all HTTP headers from untrusted sources to eliminate `\r\n` .

References

https://hackerone.com/reports/409943
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12116

For more information

If you have any questions or comments about this advisory:

- Open an issue in undici repository
- To make a report, follow the SECURITY document

Severity

Moderate 5.3 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	Low
Availability	None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVE ID

CVE-2022-31150

Weaknesses

CWE-93

Credits

Haxatron