CRLF Injection in Nodejs ‘undici’ via Content-Type

Moderate **mcollina** published **GHSA-f772-66g8-q5h3** on Aug 9

Package

undici (npm)

Affected versions	Patched versions
=< 5.8.1	5.8.2

Description

Impact

`=< undici@5.8.0` users are vulnerable to *CRLF Injection* on headers when using unsanitized input as request headers, more specifically, inside the `content-type` header.

Example:

```
import { request } from 'undici'

const unsanitizedContentTypeInput =  'application/json\r\n\r\nGET /foo2 HTTP/1.1'

await request('http://localhost:3000, {
    method: 'GET',
    headers: {
      'content-type': unsanitizedContentTypeInput
    },
})
```

The above snippet will perform two requests in a single `request` API call:

1. `http://localhost:3000/`
2. `http://localhost:3000/foo2`

Patches

This issue was patched in Undici v5.8.1

Workarounds

Sanitize input when sending content-type headers using user input.

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-2022-35948

Weaknesses

CWE-93

Credits

happyhacking-k