Hostname Spoofing in ionicabizau/parse-url

0

Valid Reported on Aug 7th 2022

Description

parse-url parses following http(s) url incorrectly, identifies its protocol as ssh, and its host name is parsed incorrectly either.

```
https://www.google.com:x@fakesite.com:x
```

```
# node -e 'const parseUrl=require("parse-url");console.log(parseUrl("https:
{
  protocols: [ 'ssh' ],
  protocol: 'ssh',
  port: '',
  resource: 'www.google.com',
  host: 'www.google.com',
  user: 'git',
  password: '',
  pathname: '/x',
  hash: '',
  search: '',
  href: 'https://www.google.com:x@fakesite.com:x',
  query: {},
  parse_failed: false
}
```

But url library parses correctly.

```
# node -e 'const url=require("url");console.log(url.parse("
Url {
  protocol: 'https:'
```

```
  protocol: 'https:',
  slashes: true,
  auth: 'www.google.com:x',
  host: 'fakesite.com',
  port: null,
  hostname: 'fakesite.com',
  hash: null,
  search: null,
  query: null,
  pathname: '/:x',
  path: '/:x',
  href: 'https://www.google.com:x@fakesite.com/:x'
}
```

This may lead to bypass the hostname whitelist， attacker could do phishing attack.

Proof of Concept

Consider the following attack scenario, developer uses `parse-url` library to check whether url hostname is `www.google.com` or not, and uses `url` library to do redirect action.
If attacker constructs malformed url, then the user will be redirected to a phishing site.

```
// PoC.js
const parseUrl = require("parse-url");
const Url = require("url");

const express = require('express');
const app = express();

var url = "https://www.google.com:x@fakesite.com:x";
parsed = parseUrl(url);
console.log("[*]`parse-url` output: ")
console.log(parsed);

parsed2 = Url.parse(url);
console.log("[*]`url` output: ")
console.log(parsed2)

app.get('/', (req, res) => {
    if (parsed.host == "www.google.com") {
```

```
    if (parsed.host == "www.google.com") {
        res.send("<a href=\'" + parsed2.href + "\'>CLICK ME!</a>")
    }

})

app.listen(8888,"0.0.0.0");
```

Impact

This leads to bypass the hostname whitelist，attacker could do phishing attack and steal sensitive information.

CVE
CVE-2022-3224
(Published)

Vulnerability Type
CWE-115: Misinterpretation of Input

Severity
Critical (9.4)

Registry
Npm

Affected Version
8.0.0

Visibility
Public

Status
Fixed

Found by

Automne
@ce-automne
unranked

Fixed by

Ionică Bizău (Johnny B.)
@ionicabizau
unranked

This report was seen 1,074 times.

We are processing your report and will contact the **ionicabizau/parse-url** team within 24 hours. 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. 3 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.) modified the Severity from High (7.3) to Critical (9.4) 3 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

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

Thank you for this finding!

Automne has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Automne 3 months ago Researcher

Many thanks

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 [illegible] days. 3 months ago

Automne 3 months ago Researcher

@Ionică Bizău (Johnny B.), hi, any updates?

> 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 **9cacf3** 2 months ago
>
> **Ionică Bizău (Johnny B.)** has been awarded the fix bounty ✔
>
> This vulnerability will not receive a CVE ✖

Ionică 2 months ago Maintainer

@Automne Not sure why the disclosure bounty got reset to $0...
Thank you very much for this finding.

Automne 2 months ago Researcher

@admin, what's wrong with the disclosure bounty? why it displays as $0 there...

Jamie Slome 2 months ago Admin

As mentioned by Adam over e-mail, the bounties were withdrawn for this project prior to the vulnerability being deemed valid. We're hoping to post new bounties soon.

Ionică 2 months ago Maintainer

@admin Why were the bounties withdrawn for this project? After the call with one of the members of the Huntr staff (couple of months ago), I was encouraged to keep the project as active as possible and I tried that...

Adam Nygate 2 months ago Admin

Hi Ionică Bizău, rest assured that is not a reflection on you or the project. We're renegotiating terms with the organisation that was sponsoring your project, will be able to fund more security maintenance in the near future.

Jamie Slome 2 months ago Admin

@ionicabizau - are you happy for us to assign and publish a CVE for this report?

The researcher has requested one :)

Ionică 2 months ago Maintainer

@JamieSlome Sure, that works!

If I am not wrong the bounty reset to 0 when I changed the Severity from High (7.3) to Critical (9.4). I am wondering now if it would have been resetting without that change...

Sign in to join this conversation