6 [url-parse] Improper Validation and Sanitization

Share:

TIMELINE

onperris submitted a report to Node.js third-party modules. Feb 14th (4 years ago)

> NOTE! Thanks for submitting a report! Please replace *all* the [square] sections below with the pertinent details. Remember, the more detail you provide, the easier it is for us to triage and respond quickly, so be sure to take your time filling out the report!

I would like to report Improper Validation and Sanitization in url-parse.

It allows attacker-controlled URL values to bypass validation and sanitization.

Module

module name: url-parse
version: 1.4.4
npm page: `https://www.npmjs.com/package/url-parse`

Module Description

The url-parse method exposes two different API interfaces. The url interface that you know from Node.js and the new URL interface that is available in the latest browsers.

Module Stats

> Replace stats below with numbers from npm's module page:

5,544,078 downloads in the last week

Vulnerability

Vulnerability Description

When using url-parse in the browser the protocol of the URL returned by the parser is not validated correctly. In the Node.js environment strings like, ` javascript:` return and empty string on the resulting URL object, but in the browser the current `document.location.protocol` is used when the provided URL doesn't match the validation expression `/^([a-z][a-z0-9.+-]*:)?(\/\/)?([\S\s]*)/i`.

Steps To Reproduce:

Add the following `test to test/test.js` and run `npm run test-browser`.

```
assume(parse.extractProtocol(' javscript:')).eql({
slashes: false,
protocol: '',
rest: ''
})
```

Wrap up

Line 199 in index.js is setting the protocol to location.protocol, this is probably not the right move.

url protocol = extracted.protocol || location.protocol || '';

> Select Y or N for the following statements:

- I contacted the maintainer to let them know: [Y]
- I opened an issue in the related repository: [N]

Impact

Bypass input sanitization and validation.

OT: vdeturckheim_dev posted a comment. Feb 14th (4 years ago)

Hello,
Thanks for reporting this to us. Someone will quickly look at this report and triage it.

ronperris changed the scope from **url-parse** to **None**. Mar 1st (4 years ago)

ronperris changed the scope from **None** to **url-parse**. Mar 1st (4 years ago)

ronperris changed the status to **Triaged**. Mar 1st (4 years ago)

ronperris changed the report title from **Improper Validation and Sanitization** to **[url-parse] Improper Validation and Sanitization**. Mar 8th (4 years ago)

3rdeden joined this report as a participant. Apr 3rd (4 years ago)

3rdeden posted a comment. Apr 3rd (4 years ago)

I have a patch working for this, which basically just trims() all input before it's parsed but it's breaking one of the existing tests that explicity wants unicode whitespace at the end of the URL. An alternate fix would just do a trim left so the whitespace infront of the protocol would be trimmed creating the desired result again.

ronperris posted a comment.

Should be resolved in url-parse@1.4.5

- Referenced git commit: https://github.com/unshiftio/url-parse/commit/3ecd256f127c3ada36a84d9b8dd3ebd14316274b with the fix.

○ marcinhoppe Node.js third-party modules staff updated the severity to Critical (9.1). Jan 24th (3 years ago)

○ marcinhoppe Node.js third-party modules staff updated the severity from Critical (9.1) to High (7.3). Jan 24th (3 years ago)

○ marcinhoppe Node.js third-party modules staff added weakness "Improper Input Validation". Jan 27th (3 years ago)

○ marcinhoppe Node.js third-party modules staff closed the report and changed the status to ● **Resolved**. Jan 27th (3 years ago)

○ marcinhoppe Node.js third-party modules staff requested to disclose this report. Jan 27th (3 years ago)

○ marcinhoppe Node.js third-party modules staff disclosed this report. Jan 27th (3 years ago)