Hostname Spoofing In Url-Parse

JAVASCRIPT IMPROPER VALIDATION SPOOFING NPM

Yaniv Nizry Feb 18, 2021

Details Overview

Summary

Affected versions of url-parse mishandles certain uses of backslash such as `http:\/` and interprets the URI as a relative path. Browsers accept backslashes after the protocol, and treat it as a normal slash, while url-parse sees it as a relative path. The vulnerability fix was pushed to 1.5.0 but caused other problems, version 1.5.1 is the recommended update.

Product

url-parse before 1.5.0.

Impact

Depending on library usage and attacker intent, impacts may include allow/block list bypasses, SSRF attacks, open redirects, or other undesired behavior.

Steps To Reproduce

```
var Url = require('url-parse');
new Url('https:\\/github.com/foo/bar');
```

Expected Result:

the url would be relative without a hostname:

```
{
  slashes: false,
  protocol: 'https:',
  hash: '',
  query: '',
  pathname: '//github.com/foo/bar',
  auth: '',
  host: '',
  port: '',
  hostname: '',
  password: '',
  username: '',
  origin: 'null',
  href: 'https://github.com/foo/bar'
}
```

Remediation

Update url-parse dependency to 1.5.1 or above.

Credit

This issue was discovered and reported by Checkmarx SCA Security Researcher Yaniv Nizry.

Resources

1. Commit d1e7e88
2. Pull request
3. Security notes