Snyk Vulnerability Database › npm › url-js

Improper Input Validation

Affecting url-js package, versions <2.1.0

4.3
MEDIUM

Snyk CVSS

Exploit Maturity	**Proof of concept** ❓
Attack Complexity	**Low** ❓

See more

INTRODUCED: 28 FEB 2022   CVE-2022-25839 ❓
CWE-20 ❓   FIRST ADDED BY SNYK

Share ⌄

> NVD   5.3 MEDIUM

How to fix?

Upgrade `url-js` to version 2.1.0 or higher.

Overview

url-js is a Simple URL parser, similar to DOM URL

Affected versions of this package are vulnerable to Improper Input Validation due to improper parsing, which makes it is possible for the hostname to be spoofed. `http://\\\\\\\\\localhost` and `http://localhost` are the same URL. However, the hostname is not parsed as localhost, and the backslash is reflected as it is.
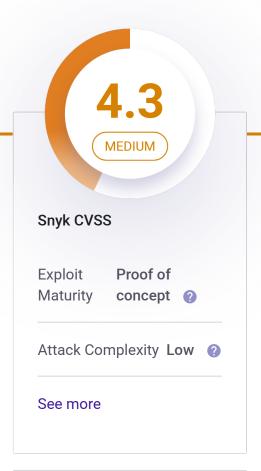
PoC:

Running the following command:

```
node -e "const URLJS = require('url-js');console.log(URLJS('http://\\\\localhost'))"
```

Will result in the following output:

```
URLJS { protocol: 'http:', username: '', password: '',
hostname: '\\localhost', port: '', pathname: '/', search:
```

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

```
'', query: '', hash: '' }
```

References

- Fix Commit

Report a new vulnerability

Found a mistake?

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon   Join the >>
community