snyk Vulnerability DB

Snyk Vulnerability Database > npm > url-js

Improper Input Validation

Affecting url-js package, versions <2.1.0

INTRODUCED: 28 FEB 2022 CVE-2022-25839 ? Share V

CWE-20 ? FIRST ADDED BY SNYK

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:

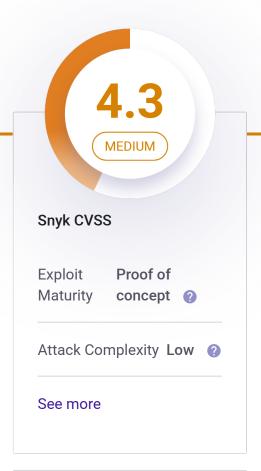
Running the following command:

```
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:
```

Q Search by package n





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

Snyk SNYK-JS-URLJS-ID 2414030

Published 7 Mar 2022

Disclosed 28 Feb 2022

Credit Pocas

Report a new vulnerability

Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

Jobs
Contact
Policies
Do Not Sell My Personal Information
CONTACT US
Support
Report a new vuln
Press Kit
Events

About

FIND US ONLINE

TRACK OUR DEVELOPMENT



© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.