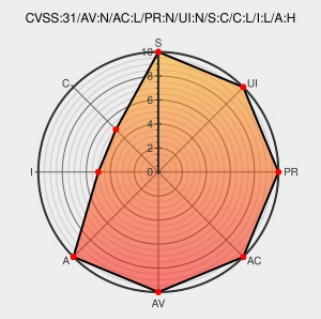
CVE-2020-7741

Published on: 10/06/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7741

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Hello.js from Hello.js Project contain the following vulnerability:

This affects the package hellojs before 1.18.6. The code get the param oauth_redirect from url and pass it to location.assign without any check and sanitisation. So we can simply pass some XSS payloads into the url param oauth_redirect, such as javascript:alert(1).

CVE-2020-7741 has been assigned by report@snyk.io to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.9 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
fix(xss): oauth_redirect should be a valid url · MrSwitch/hello.js@d6f5137 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/MrSwitch/hello.js/commit/d6f5137f30de6e0ef70

Cross-site Scripting (XSS) in hellojs | Snyk	Third Party Advisory snyk.io text/html	MISC snyk.io/vuln/SNYK-JS-HELLOJS-1014546
hello.js/hello.all.js at 3b79ec93781b3d7b9c0b56f598e060301d1f3e73 · MrSwitch/hello.js · GitHub	Broken Link github.com text/html	MISC github.com/MrSwitch/hello.js/blob/3b79ec93781b3d7b9c0b56f598e0

Related QID Numbers

983715 Nodejs (npm) Security Update for hellojs (GHSA-7jh9-6cpf-h4m7)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hello.js Project	Hello.js	All	All	All	All
Application	Hello.js Project	Hello.js	All	All	All	All

cpe:2.3:a:hello.js_project:hello.js:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:hello.js_project:hello.js:*:*:*:*:*:node.js:*:*:

Discovery Credit

Anonymous Reporter

← Previous ID

Next ID→