

Cross-site Scripting (XSS)

Affecting jquery package, versions <1.9.1

INTRODUCED: 19 MAY 2020 CVE-2020-7656 CWE-79 FIRST ADDED BY SNYK Share

How to fix?

Upgrade jquery to version 1.9.1 or higher.

Overview

jquery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.

Affected versions of this package are vulnerable to Cross-site Scripting (XSS). load() fails to recognize and remove " <script> " HTML tags that contain a whitespace character, i.e. " </script > " which results in the enclosed script logic to be executed. This can lead to Cross-site Scripting attacks when an attacker has control of the enclosed script.

PoC by Robert McLaughlin

index.html:

```
<html> <head> <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/1.8.3/jquery.js"></script>
</head> <body> <div id="mydiv"></div> <script> $("#mydiv").load('inject.html #himom'); </script> </body>
</html>
```

inject.html:

```
<div id="himom"><script>alert('Arbitrary Code Execution');</script> </div>
```

References

- GitHub Additional Information

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

MEDIUM

Search by package name or CVE

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
User Interaction	Required

See more

> Red Hat	5.4 MEDIUM
> NVD	6.1 MEDIUM

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

Snyk Learn

Learn about Cross-site Scripting (XSS) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-JQUERY-569619
Published	19 May 2020
Disclosed	19 May 2020
Credit	Robert McLaughlin

Report a new vulnerability Found a mistake?

[Documentation](#)

[Disclosed Vulnerabilities](#)

[Blog](#)

[FAQs](#)

#### COMPANY

[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



© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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