snyk Vulnerability DB

Snyk Vulnerability Database › Maven ›
io.socket:socket.io-client

Search by package n

NULL Pointer Dereference

Affecting io.socket:socket.io-client package, versions [,2.0.1)

INTRODUCED: 10 JUL 2022 CVE-2022-25867 ?
CWE-476 ? FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `io.socket:socket.io-client` to version 2.0.1 or higher.

Overview

Affected versions of this package are vulnerable to NULL Pointer Dereference when parsing a packet with with invalid payload format.

References

- GitHub Commit
- GitHub Commit
- GitHub Issue
- GitHub Release

7.5

HIGH

Snyk CVSS

Exploit Maturity	**Proof of concept**	?
Attack Complexity	**Low**	?
Availability	HIGH	?

See more

› **NVD** 7.5 HIGH

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 suggest you quick fixes.

Test your applications

Snyk ID	**SNYK-JAVA-IOSOCKET-2949738**
Published	**1 Aug 2022**
Disclosed	**10 Jul 2022**
Credit	**Andrei Nikonov**

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

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

Registered in England and Wales. Company number: 09677925

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