

Command Injection

Affecting madge package, versions <4.0.1

INTRODUCED: 5 MAR 2021 CVE-2021-23352 CWE-89 FIRST ADDED BY SNYK Share

How to fix?

Upgrade madge to version 4.0.1 or higher.

Overview

madge is a Madge is a developer tool for generating a visual graph of your module dependencies, finding circular dependencies, and give you other useful info.

Affected versions of this package are vulnerable to Command Injection. It is possible to specify a custom Graphviz path via the graphVizPath option parameter which when the .image(), .svg() or .dot() functions are called, is executed by the childprocess.exec function.

PoC

```
1. install 'madge' module: 'npm i madge' 2. run the following poc.js:
// Example taken from: https://github.com/pahen/madge#svg

const madge = require('madge'); madge('..', {graphVizPath: "touch HELLO;"}) .then((res) => res.svg())
.then((writtenImagePath) => { console.log('Image written to ' + writtenImagePath); });
```

References

- GitHub Commit
- Vulnerable Code

PRODUCT

- Snyk Open Source
- Snyk Code
- Snyk Container
- Snyk Infrastructure as Code
- Test with Github
- Test with CLI

RESOURCES

- Vulnerability DB
- Documentation
- Disclosed Vulnerabilities

HIGH

Search by package name or CVE

Snyk CVSS

Exploit Maturity	Mature
Attack Complexity	Low
Confidentiality	HIGH

See more

> NVD 9.8 CRITICAL

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 Command Injection vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-MADGE-1082875
Published	9 Mar 2021
Disclosed	5 Mar 2021
Credit	Alessio Della Libera (d3lla)

Report a new vulnerability

Found a mistake?

[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.