Arbitrary Code Execution

Affecting node-rules package, versions **>=3.0.0 <5.0.0**

INTRODUCED: 10 MAR 2020 CVE-2020-7609 CWE-78 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `node-rules` to version 5.0.0 or higher.

Overview

node-rules is a light weight forward chaining Rule Engine, written in JavaScript.

Affected versions of this package are vulnerable to Arbitrary Code Execution. The injection point is located in line 152,153. The argument rules of function `fromJSON()` can be controlled by users without any sanitization.

Proof Of Concept

```
var A = require("node-rules"); var rules = { condition:"{}.__proto__.toString = 123", consequence:"console.log(123)" } var a = new A(); a.fromJSON(rules); console.log({}.toString)
```

References

- GitHub Fix Commit
- GitHub Issue

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
Scope	Changed
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-JS-NODERULES-560426
Published	17 Mar 2020
Disclosed	10 Mar 2020
Credit	JHU System Security Lab

Report a new vulnerability | Found a mistake?