VM2 Sandbox Breakout Through __lookupGetter__

Critical **patriksimek** published **GHSA-grj5-jjm8-h35p** 3 days ago

Package

vm2 (npm)

Affected versions

<= 3.10.4

Patched versions

3.11.0

Description

Summary

VM2 suffers from a sandbox breakout vulnerability. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system.

Details

The `__lookupGetter__` method allows to read the getter of an object. It is special in VM2 since it will switch between the host and sandbox version of the method when passed to the other context.
This allows to access getters on an object in the host context if the method is called from the host context which can be achieved by using the host `apply` method which can be accessed through `Buffer.apply`.
Afterwards, this function can be used to call the host version of `__lookupGetter__` with `Buffer` and `__proto__` resulting in the prototype lookup method from the host context.
With this method the hosts `Function.prototype` object can be retrieved and the host `Function` acquired through the `constructor` property which allows to create and run code in the host context.
This issue was attempted to be fixed with

vm2/lib/bridge.js
Line 427 in 4b009c2

```
427     if (desc.value && desc.value.name === 'Function') return {};
```

. However, this can be circumvented by using `Object.getOwnPropertyDescriptor` to get the `constructor` property.

PoC

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

```
const {VM} = require("vm2");
const vm = new VM();
vm.run(`
const g = ({}).__lookupGetter__;
const a = Buffer.apply;
const p = a.apply(g, [Buffer, ['__proto__']]);
Object.getOwnPropertyDescriptor(p.call(a),'constructor').value('return process')().mainM
`);
```

Impact

Attackers can perform Remote Code Execution under the assumption that arbitrary code can be executed 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-2026-24118

Weaknesses

No CWEs

Credits

XmiliaH Reporter