TOTOLINK Vulnerability

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

漏洞描述

Totolink outdoor CP900 V6.3c.566_B20171026版本。通过webWlanIdx参数在setWebWlanIdx函数中包含命令注入漏洞。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 setWebWlanIdx(int a1, int a2, int a3)
{
  const char *Var; // $v0
  char v7[64]; // [sp+1Ch] [-48h] BYREF

  Var = (const char *)websGetVar(a2, "webWlanIdx", "0");
  sprintf(v7, "echo %s > /tmp/webWlanIdx", Var);
  CsteSystem(v7, 0);
  websSetCfgResponse(a1, a3, "0", "reserv");
  return 0;
}
```

POC