TALOS-2021-1330

Lantronix PremierWave 2050 Web Manager FSBrowsePage directory traversal vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21886

Summary

A directory traversal vulnerability exists in the Web Manager FSBrowsePage functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially crafted HTTP request can lead to information disclosure. 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

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

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, but unprivileged, user to browse a subset of the device’s filesystem, rooted at `/ltrx_user/`. The system attempts to limit the user from browsing outisde of the `/ltrx_user/` directory by prepending all file paths with `/ltrx_user/`. Depending on the functionality being exercised (open file, copy file, move file, etc.) path traversal sanitization will be applied to some of the HTTP parameters prior to their use. One of the features exposed through this interface can be exploited to allow a user to view directory listings for arbitrary directories by means of an unsanitized path traversal vulnerability.

An attacker-controlled HTTP parameter, `dir`, can be altered to include path traversal primitives which will not be sanitized before being used to compose the final directory path. By submitting `/../` as the start of the `dir` field an authenticated attacker can escape `/ltrx_user/` and navigate the file system from the root directory. It is important to note that the logic which allows a user to view the contents of files requires that the file being viewed must be a child of the `/ltrx_user/` directory, and viewing files outside of this directory results in a `400 Bad Request: unknown file` error response. Therefore, this vulnerability is limited to disclosing file and directory names.

The below request will disclose a directory listing of `/etc/`.

```
POST / HTTP/1.1
Host: [IP]:[PORT]
Content-Length: 26
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=FsBrowsePage&dir=/../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.

VULNERABILITY REPORTS

PREVIOUS REPORT
TALOS-2021-1329

NEXT REPORT
TALOS-2021-1331