Talos Vulnerability Report

TALOS-2021-1322

Lantronix PremierWave 2050 Web Manager Applications and FsBrowse local file inclusion vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21878

Summary

A local file inclusion vulnerability exists in the Web Manager Applications and FsBrowse functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted series of HTTP requests can lead to local file inclusion. An attacker can make a series of authenticated HTTP requests 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:H/I:N/A:N

CWE

CWE-668 - Exposure of Resource to Wrong Sphere

Details

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

The PremierWave 2050 provides its users the ability to upload and execute arbitrary python scripts. This functionality is accessible via the `Administration > Applications` interface of the Web Manager site. The device executes these scripts as a low-privilege user named `default`. Permissions are appropriately reduced via `setuid` and `setgid` before executing the script.

Executing the following python script will fail, as expected, due to a permission error.

```
print(open('/etc/shadow', 'r').read())
```

However, an authorization mismatch exists between the privileges used when executing python applications and the privileges used when browsing the file system via the `Filesystem > Browse` page. The Web Manager application does not drop privileges when interacting with the file system on behalf of the user.

Instead, an authenticated and authorized attacker can successfully execute the following python script.

```
import os
os.system('ln -s /etc/shadow ./shadow')
```

Subsequently navigating to the `Filesystem > Browse` page will allow the authenticated attacker to access the symlinked file with root privileges and disclose the contents of `/etc/shadow` or any arbitrary file.

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.
