Talos Vulnerability Report

TALOS-2022-1459

TCL LinkHub Mesh Wifi libcommonprod.so prod_change_root_passwd hard-coded password vulnerability

AUGUST 1, 2022

CVE NUMBER

CVE-2022-22144

SUMMARY

A hard-coded password vulnerability exists in the libcommonprod.so prod_change_root_passwd functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. During system startup this functionality is always called, leading to a known root password. An attacker does not have to do anything to trigger this vulnerability.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

TCL LinkHub Mesh Wifi MS1G_00_01.00_14

PRODUCT URLS

LinkHub Mesh Wifi - https://www.tcl.com/us/en/products/connected-home/linkhub/linkhub-mesh-wifi-system-3-pack

CVSSV3 SCORE

7.5 - CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE

CWE-259 - Use of Hard-coded Password

DETAILS

The LinkHub Mesh Wi-Fi system is a node-based mesh system designed for Wi-Fi deployments across large homes. These nodes include most features standard in current Wi-Fi solutions and allow for easy expansion of the system by adding nodes. The mesh is managed solely by a phone application, and the routers have no web-based management console.

During the boot process of the device, the `netctrl` binary is launched. Within `main` the function `prod_change_root_passwd` is called from `libcommonprod` with no conditional checks to do so. This function forces a change of the root password to `tcl-wifi` as seen below.

```
int32_t prod_change_root_passwd()
    void var_d4
    memset(&var_d4, 0, 0x40)
    int32_t var_94 = 0
    int32_t var_90 = 0
    void var_8c
    memset(&var_8c, 0, 0x80)
    int32_t var_d8 = 0
    memcpy(&var_8c, "tcl-wifi", 9)
    doSystemCmd("(echo %s;sleep 1;echo %s) | pass…", &var_8c, &var_8c)     [1]
    return 0
```

The forced password change occurs at [1] when `tcl-wifi` is passed into the `passwd` command line utility.

TIMELINE

2022-04-27 - Vendor Disclosure
2022-08-01 - Public Release

CREDIT

Discovered by Carl Hurd of Cisco Talos.

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