CVE-2020-28055 - TCL Android Smart TV (All) - Incorrect Permission Assignment for Critical Vendor Resources - TCL Android TV Vendor Configuration & Upgrade Folders World Writable to Local Attacker

CVE-2020-28055 - TCL Android Smart TV (All) - Incorrect Permission Assignment for Critical Vendor Resources - TCL Android TV Vendor Configuration & Upgrade Folders World Writable to Local Attacker

by Sick Codes — November 9, 2020 - Updated on December 31, 2020 in Security 1

TCL TV Vulnerability CVE-2020-28055

Title

TCL Android Smart TV (All) - Incorrect Permission Assignment for Critical Vendor Resources - TCL Android TV Vendor Configuration & Upgrade Folders World Writable to Local Attacker

CVE ID

CVE-2020-28055

CVSS Score

7.8

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Internal ID

SICK-2020-012

Vendor

TCL Technology Group Corporation

Product

TCL Android Smart TV Firmware (All)

Product Versions:

V8-R851T02-LF1 V295 and below

Many models affected (untested)

Vulnerability Details

A vulnerability in the TCL Android Smart TV series by TCL Technology Group Corporation allows a local unprivileged attacker, such as a malicious App, to read and write to critical vendor resource directories within the Android TV file system, including the vendor upgrades folder.

The following three critical resource folders are assigned permissions of 0777 by the vendor rc file located at /system/vendor/etc/init/hw/init.rtd285o.rc from line 344:

/data/vendor/tcl

/data/vendor/upgrade

/var/TerminalManager

This allows a local unprivileged user, or a malicious APK, to modify critical system resources. For example, by modifying the /data/vendor/upgrade folder, an attacker could potentially cause the Android TV to undergo arbitrary vendor system upgrades.

Vendor Response

None.

Credits

- @sickcodes - https://twitter.com/sickcodes/ vulnerability discovery & initial report
- @johnjhacking - https://twitter.com/johnjhacking/ security team engagement & PoC contribution

Disclosure Timeline

- **2020-10-29** - Researcher discovers vulnerability during reconnaissance
- **2020-10-29** - Vendor notified via email
- **2020-11-02** - CVE assigned CVE-2020-28055
- **2020-11-08** - Research final notifies vendor for an update
- **2020-11-10** - Researcher publishes CVE-2020-28055

References

https://github.com/sickcodes/security/blob/master/advisories/SICK-2020-012.md

https://sick.codes/sick-2020-012

https://sick.codes/extraordinary-vulnerabilities-discovered-in-tcl-android-tvs-now-worlds-3rd-largest-tv-manufacturer/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28055

https://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-28055

Mitigation

The following firmware updates do not refer to the Android system updates; updates refer to the vendor specific third-party firmware updates provided by TCL.

- Update to the latest over-the-air (OTA) vendor firmware from TCL.

Or

- Update to the latest vendor firmware from the TCL website using a USB drive and the firmware update method for your model.

TCL Android Smart TVs cannot be manually patched without root user access (rooted).

TCL Smart TVs that are not rooted cannot be manually updated other than using OTA or USB update methods.

Offline TVs are low risk because there are no attackers on the adjacent network.

If your TV is in a high-risk environment, and you are unable to update the vendor firmware, it is recommended to disable internet access on the TCL Android TV until patched.

Manual or offline TV updates require elevated permissions to fix this vulnerability and cannot be patched without root user access:

```
chmod 0770 /data/vendor/tcl /data/vendor/upgrade /var/TerminalManager
```

Comments 1

Maui 11 months ago

My TCL was hack and til now unable to remove the app that was installed since they got my IP add and all the credentials log in on my email kindly help me out call me at [REDACTED] dont have access to my emails

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

Privacy - Terms

I am human

POST COMMENT

@sickcodes

@sickcodes

@sickcodes

Discord Server

sickcodes.slack.com

t.me/sickcodeschat

./contact_form