sickcodes [CVE-2020-28055] 7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H ✓ History

1 contributor

98 lines (57 sloc) | 3.57 KB

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

V8-T658T01-LF1 V373 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

Vendor notified by email in response to .

Credits

@sickcodes - https://twitter.com/sickcodes/ discovery.

@johnjhacking - https://twitter.com/johnjhacking/ collaborator.

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://github.com/sickcodes/security/blob/master/etc/CVE-2020-27403_CVE-2020-28055_Press-Statement-and-Questions_11162020.pdf

https://github.com/sickcodes/security/blob/master/etc/CVE-2020-27403_CVE-2020-28055_GlobalFAQ.pdf

CVE Links

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 TV's cannot be manually patched without root user access (rooted).

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

Offline TV's 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
```