UPDATED PRESS STATEMENT (11-16-2020)

"TCL was recently notified by an independent security researcher of two vulnerabilities in Android TV models. Once TCL received notification, the company quickly took steps to investigate, thoroughly test, develop patches, and implement a plan to send updates to resolve the matter. Updating devices and applications to enhance security is a regular occurrence in the technology industry, and these updates should be distributed to all affected Android TV models in the coming days.

TCL takes privacy and security very seriously, and particularly appreciates the vital role that independent researchers play in the technology ecosystem. We wish to thank the security researchers for bringing this matter to our attention as we work to advance the user experience. We are committed to bringing consumers secure and robust products, and we're confident that we're putting in place effective solutions for these devices."

FAQ

Q1. Do these vulnerabilities apply to models sold in the USA or Canada?

A1. CVE-2020-24703 is not an issue in product deployed in North America. However, select televisions sold in the USA and Canada are affected by CVE-2020-28055. We expect to resolve this in the coming days.

Q2. Are all TCL televisions affected?

A2. TCL has deployed hundreds of models in North America and only a limited number are involved. The following models are impacted by CVE-2020-28055: 32S330, 40S330, 43S434, 50S434, 55S434, 65S434, and 75S434.

Q3. When was TCL made aware of these vulnerabilities?

A3. The TCL lab was made aware of the discovery at 11:30am on October 27. Within hours, the issues had been verified and the security compliance team triggered the vulnerability management response process. The solution for CVE-2020-27403 began deployment on October 30 via APK upgrade. The TCL lab is working around the clock to test the solution for a system upgrade to address CVE-2020-28055 to complete the modification of directory permissions. Pending successful testing, it is expected that updates will start being distributed in the coming days.

Q4. Why is CVE-2020-24703 not an issue within the North America market?

A4. This vulnerability was a result of the application T-Cast (Magic Connect) used to stream user content from a mobile device. This vulnerability allowed content directories to be viewed through the LAN, however there is no permission to write or execute. T-Cast was never installed on televisions distributed in the USA or Canada and therefore this vulnerability did not exist on those products. For those affected sets, the APK was updated to resolve this issue.

Q5. What is the liability of the /data/vendor/upgrade directory availability within CVE-2020-28055

A5. Although it has never been used, this directory exists for OAD upgrade. The execution process is that the module downloads the upgrade package into this directory. After the download is completed, it will decompress and set a flag through the interface. When the TV boots up the next time, it detects that flag and performs the upgrade. If you copy an upgrade package directly to the directory, the upgrade will not be performed. However, the coming firmware upgrade will patch this vulnerability.

Q6. What is the purpose of /var/TerminalManager?

A6. The Terminal Manager APK supports remote diagnostics in select regions. The process must be initiated by the user and a code provided to TCL customer service agents in order to perform diagnostics for the television. This functionality was never implemented in the North America market.

Q7. Does TCL have control or access to any cameras or microphones attached to the television?

A7. In areas supported by the Terminal Manager APK, TCL is able to remotely operate most functions of the television remotely ONLY if the user requests such action during the diagnostic session. The process must be initiated by the user and a code provided to TCL customer service agents in order to have diagnostic access to the television. This functionality was never implemented in the North America market.

Q8. What is the purpose of /data/vendor/tcl?

A8. This folder is present to store advertising graphics. The televisions have the capability to display an ad as part of the boot-up process. We do not currently utilize boot ads in these devices and therefore the folder is unused. While this folder is currently visible, no write or execution permissions are granted.

Q9. What efforts are being undertaken to ensure that future models are more secure?

A9. TCL has always followed industry-standard testing. Additionally, TCL has partnered with 3rd party security firms to perform further robust penetration testing for all new chassis designs and firmware executions. Going forward, we are putting processes in place to better react to discoveries by 3rd parties. These real-world experts are sometimes able to find vulnerabilities that are missed by testing. We are performing additional training for our customer service agents on escalation procedures on these issues as well as establishing a direct reporting system online.