Media Q&As

1. **Are all TCL televisions affected?**
TCL has been made aware of two vulnerabilities (‘CVE-2020-27403’ and ‘CVE-2020-28055’) that are peculiar to particular TCL’s Android TV models. TCL has already found a solution to vulnerability ‘CVE-2020-27403’ and began deployment of a security patch to fix the problem on October 30 via APK upgrade. Vulnerability ‘CVE-2020-28055’ affects many Android TV models and TCL lab is working around the clock to test the solution for a system upgrade to address the vulnerability. Pending successful testing, it is expected that updates will start being distributed in the coming days.

2. **Who made this discovery?**
The discovery was made by two industry researchers @sickcodes and @johnjhacking.

3. **When was TCL made aware of these vulnerabilities?**
The TCL lab was made aware of the discovery, by researchers @sickcodes and @johnjhacking, 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.

4. **What is CVE-2020-24703 vulnerability?**
This vulnerability was a result of the application T-Cast (Magic Connect) used to stream user content from a mobile device. This vulnerability allowed the filesystem to be viewed through the LAN, however there is no permission to write or execute. For those affected sets, the APK was updated to resolve this issue.

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

6. **What is the purpose of /var/TerminalManager?**
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.

6.1 Does TCL have control or access to any cameras or microphones attached to the television?
In areas supported by the Terminal Manager APK, TCL is able to remotely operate relevant 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.

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

This folder helps televisions 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.

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

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, such as Researchers, who 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.

9. Will you recall any products? In which markets? What's the financial implication? What's the timeline?

We do not have any plans to recall any products. 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.

10. Does it affect your plan to roll out other products in the near term?

No. We are committed to bringing consumers secure and robust products, and we're confident that we're putting in place effective solutions for these and future devices.

11. It has been reported that the problem was fixed using a 'silent patch' whereby TCL remotely logged in to the user's (Sick Codes') TV to resolve the issue. Has the patch also been installed on other affected devices?

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. We are committed to bringing consumers secure and robust products, and we're confident that we're putting in place effective solutions for these and future devices.

12. Is this the first time that this sort of thing has happened?

TCL has always followed industry-standard testing. The company partners with 3rd party security firms to perform robust penetration testing for all new chassis designs and firmware executions and welcomes discoveries by 3rd parties, such as Researchers, who are sometimes able to find vulnerabilities that are missed in the testing process.

13. **Are all TCL Smart TV owners vulnerable? Could it be that other TCL TV owners have had their information compromised?**

This issue is peculiar to particular TCL's Android TV models and we have no indication that any unauthorized access occurred apart from the initial discovery. 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.

14. Have all TCL Android TV's had a patch installed? Are all TCL Android TV's now safe?

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.

15. Why was this loophole not identified by the technical team in first place? Has TCL made sure that there are no further loopholes? What measures will be taken to stop it happening again?

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, such as Researchers, who 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.