sickcodes [CVE-2020-27403] 6.5 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N History

1 contributor

132 lines (92 sloc) | 5.95 KB

Title

TCL Android Smart TV (All) - Exposure of Information Through Directory Listing - TCL Android TV Filesystem Browsable to Unauthenticated Attackers Over the Adjacent Network on Port 7989

CVE ID

CVE-2020-27403

CVSS Score

6.5

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

Internal ID

SICK-2020-009

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 an attacker on the adjacent network to arbitrarily browse and download sensitive files over an insecure web server running on port 7989 that lists all files & directories.

An unprivileged remote attacker on the adjacent network, can download most system files, leading to serious critical information disclosure.

For example, if the TV is assigned a local IP address of 10.0.0.2, an attacker can browse the "/proc" Linux file directory simply by visiting http://10.0.0.2:7989/proc in a web browser.

In version 373, an attacker can navigate the entire root file system by simply visiting http://10.0.0.2:7989 in a web browser.

However, in version 295, the root directory in not browsable from root ('/'). Instead, an attacker can directly visit known Android directories & files. Outside of the root directory of the filesystem, every deeper directory is browsable.

Notable directories that contain critically sensitive information, images, downloads, data, or logs include:

```
10.0.0.2:7989/proc
10.0.0.2:7989/dev
10.0.0.2:7989/sys
10.0.0.2:7989/init.rc
10.0.0.2:7989/mnt/sdcard/Download
10.0.0.2:7989/mnt/sdcard/DCIM
10.0.0.2:7989/cache
10.0.0.2:7989/root
10.0.0.2:7989/oem
10.0.0.2:7989/tmp
10.0.0.2:7989/userdata
10.0.0.2:7989/vendor
```

Credits

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

Vendor Response

Vendor allegedly patched & performed silent update.

Disclosure Timeline

- **2020-10-16** - Researcher discovers vulnerability
- **2020-10-16** - Researcher submits contact form at Vendor website
- **2020-10-17** - Researcher direct messages (DM) Vendor via Twitter
- **2020-10-17** - Researcher inboxes Vendor via Email
- **2020-10-17** - Researcher chats to customer support of Vendor via Live Chat
- **2020-10-17** - Researcher requests CVE
- **2020-10-20** - Researcher DM's Vendor's other Twitter
- **2020-10-18** - Researcher requests CVE from Open Handset Alliance CNA (Google) instead
- **2020-10-19** - Researcher phones Customer Support request to forward report to the security/engineering team
- **2020-10-20** - Researcher phones Customer Support again emphasizing the urgency
- **2020-10-20** - Researcher posts on https://community.disclose.io asking for a contact for the security team at vendor
- **2020-10-20** - Researcher DM's Vendor's other Twitter
- **2020-10-21** - Another researcher supplies contact details within Vendor and researcher emails said contact
- **2020-10-21** - Vendor's Customer Support replies to ticket 2020-10-16 requesting product model (already given the ticket)
- **2020-10-21** - Researcher forwards email to security contact within vendor
- **2020-10-21** - Researcher forwards email to another security contact within vendor
- **2020-10-21** - Researcher DM's Vendor 4x Twitter accounts
- **2020-10-23** - Researcher forwards email to vendor customer support
- **2020-10-23** - Researcher DM's Vendor 4x Twitter accounts
- **2020-10-24** - Researcher forwards email to Customer Privacy team at vendor
- **2020-10-24** - Researcher forwards email to Vendor partner
- **2020-10-26** - Vendor customer support replies to 2020-11-23: "someone will get in touch with you shortly"
- **2020-10-27** - Researcher forwards email to security contact within vendor
- **2020-10-28** - Vendor partner confirms unrelated to their brand
- **2020-10-28** - Researcher asks Vendor partner to forward to security team
- **2020-10-29** - Vendor finally replies and allegedly patches vulnerability on same day
- **2020-11-02** - CVE assigned CVE-2020-27403
- **2020-11-08** - Researcher confirms fix in test model
- **2020-11-08** - Research final notifies vendor for an update
- **2020-11-10** - Researcher publishes CVE-2020-27403

References

https://github.com/sickcodes/security/blob/master/advisories/SICK-2020-009.md

https://sick.codes/sick-2020-009

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-2020-27403

https://nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-27403

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.