TCL Android Smart TVs Breached By Backdoor Security Exploits Allowing Critical System Access

hothardware.com/news/tcl-tvs-are-a-cybersecurity-threat

November 13, 2020

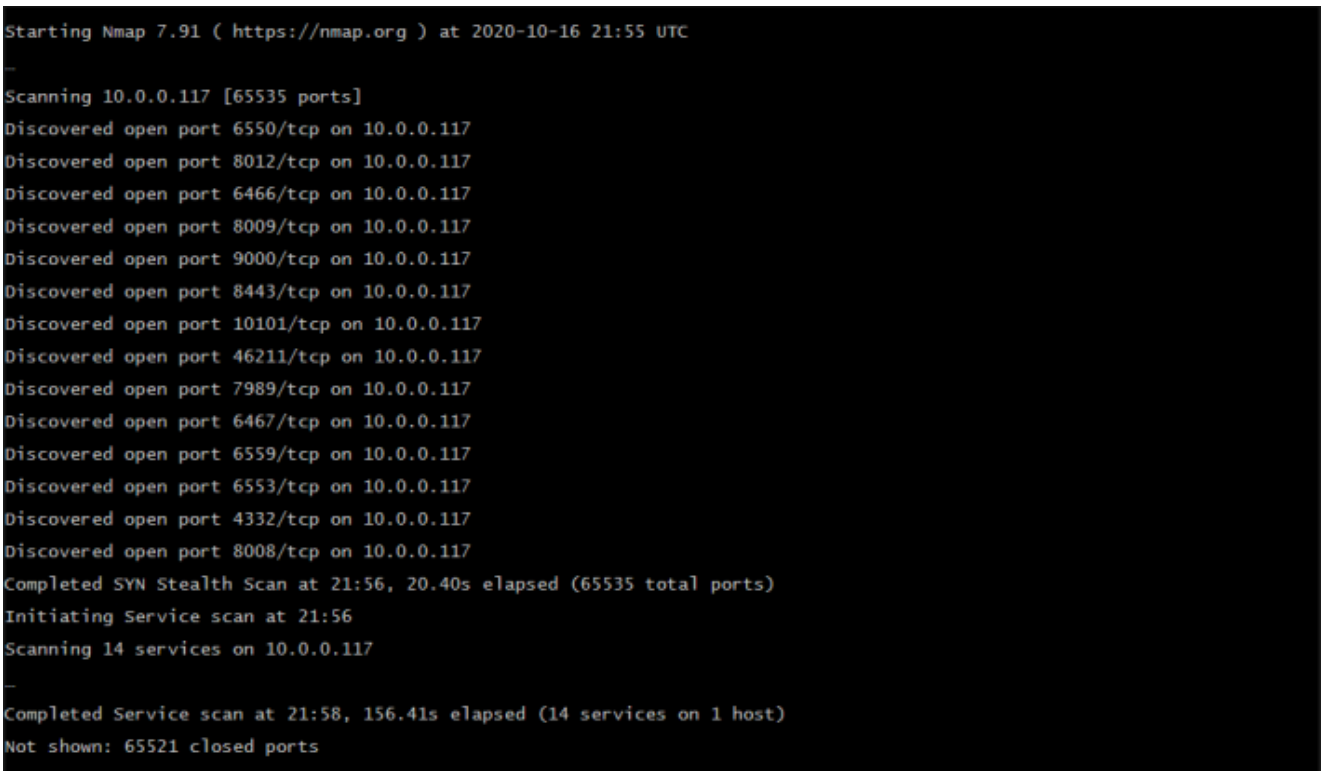
by **Nathan Ord** — Friday, November 13, 2020, 03:07 PM EDT

TCL Android TVs have been crowding retail stores since their initial launch earlier this year. The Chinese-manufactured TVs have been a “budget-option” that works well enough for most and is a steal compared to the competition. When you get a TCL 65” TV for $229, though, is cybersecurity at the top of your mind? If not, you are in for a surprise.

Security researcher and hacker SickCodes seems to be a jack-of-all-trades, continually poking at devices to see what exploits he can find. At the end of September, he looked at “low-end Android boxes,” things such as TV sticks, boxes, Smart TVs, and Android TVs. As he explains, they are all basically “like a little Raspberry Pi competitor, focusing on GPU performance through the small, but powerful, Mali GPUs.” He then explains that some of the products investigated “were “factory-flawed” and deliberately insecure.” After a conversation with a friend, SickCodes realized that Smart TVs are likely not all that different from TV sticks, so they may be susceptible to the same issues.

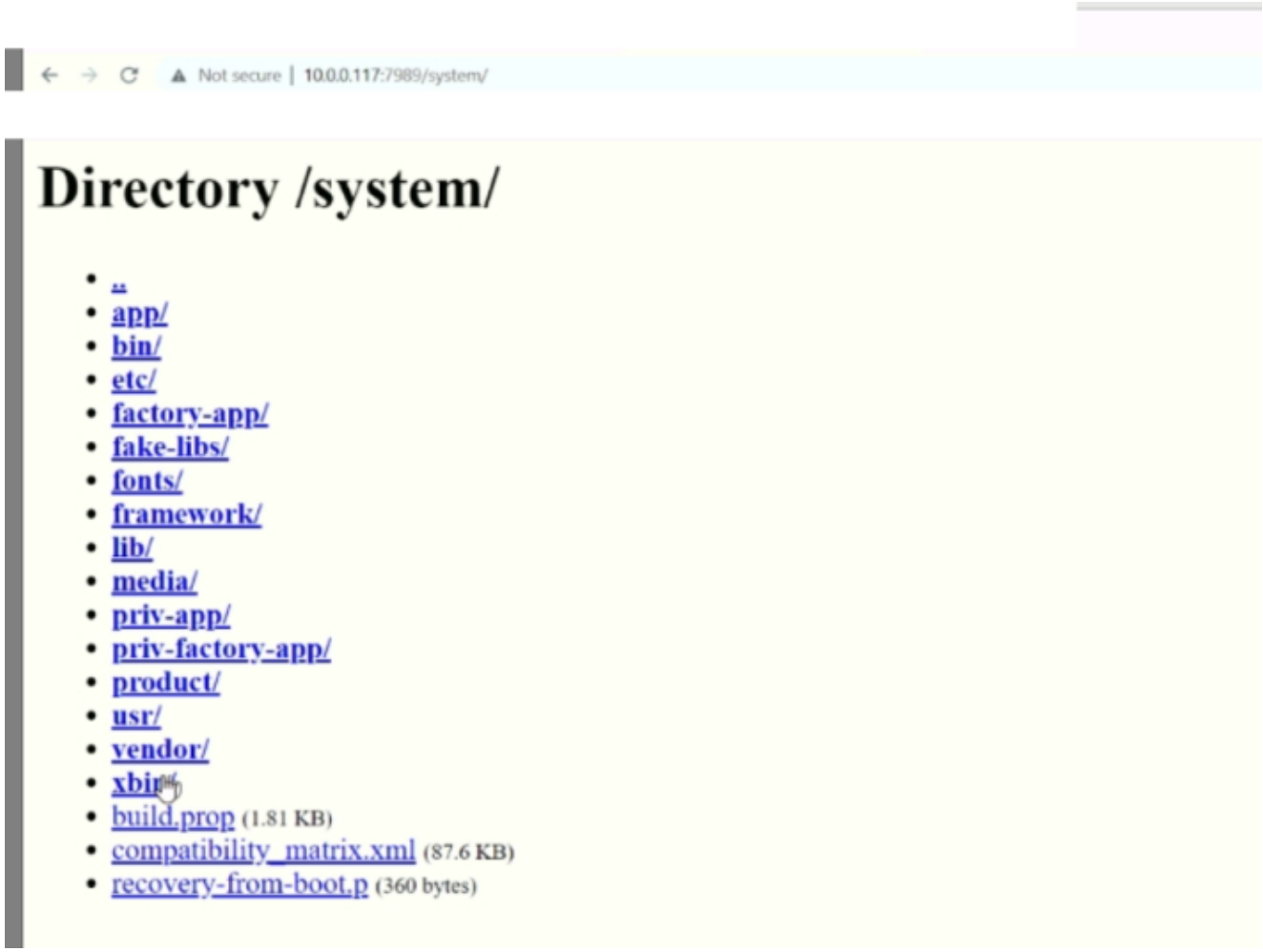
After moving on from the TV sticks and other like devices, SickCodes got his hands on a TCL TV. With just a simple scan, he found 14 different TCP ports open on the one TCL TV.

As SickCodes explains, if you scan an “Android mobile phone, you will generally find 0 open TCP ports.” While there could be reasons for open ports, there really would not be a reason for some of the services found through the scan. Thus, the TCL investigation goes a level deeper.



TCL TV Port Scan

SickCodes started to poke and prod at the individual ports he found, opening them in web browsers or scanning them with a variety of tools. Using context from prior research, he was able to poke at specific Android directories he had seen before. This is where he found the full TV filesystem exposed to the network. For any device ever, there is no reason for the full filesystem to be exposed like that. Furthermore, this open port was not one typically used and was not registered with the IANA, a group that manages what ports are regularly used. It was essentially a secret backdoor into any TV, where the possibilities were endless.



TCL TV File System

When it comes to researching security topics, if you find something, it needs to be reported to both the company who made the product and MITRE, a non-profit research organization tasked with assigning common vulnerability and exposure (CVE) numbers. SickCodes tried to do that and got no reply, so he reached out for help. Another researcher, named John Jackson, got in touch with SickCodes after he reached out. As Jackson explains, “It seemed like a legitimate issue” and “It was clear that utilizing this vulnerability could result in remote code execution or even quick network pivots with the intention of exploiting systems quickly with ransomware.” This issue needed to be made known and could not be brushed off. Unfortunately, Jackson hit the same stone wall that SickCodes did.

Terminal Manager Capabilities

After 13 days, however, TCL Corporation replied to the initial report, with it taking another two weeks for a receipt of the security report. This is from the world's second-largest TV manufacturer by TCL's claims. In the same email, the TCL Security Team also confirmed that the vulnerability was fixed. Somehow, it was an easy and silent fix for the security team. It seems that "easy" does not correspond to "good" in this case, as it led to another vulnerability. SickCodes writes that "there were critical changes made by TCL to several folders on the TV file system that should be absolutely locked down." In essence, mission-critical files on the TV were now editable by any users in the file system. As these permissions were not likely intended, it became another vulnerability given CVE-2020-28055. Furthermore, an app called "TerminalManager_Remote" was discovered, which had several functionalities that would allow for remote access to a TV through several means.

Even though the vulnerability that was first found was patched (CVE-2020-27403), it opened a whole new can of worms. It was found that TCL can silently upgrade TVs or even remotely access them if they wanted to. This means the budget TV you thought was a product might have made you a product in turn. If you are looking to buy technology on a budget, think first about why it was so cheap and what that means for security as well.