Issued 12/15/17

AT&T's DirecTV Kit has a Root Hole – and No One wants to Patch It

AT&T's DirecTV wireless kit has an embarrassing vulnerability in its firmware that can be trivially exploited by miscreants and malware to install hidden backdoors on the home network equipment, according to a security researcher. Ricky Lawshae – a DEF CON veteran and infosec guru at Trend Micro's Digital Vaccine Labs – was an AT&T U-Verse subscriber who shifted over to DirecTV, and decided to take a closer look at the service's hardware. The setup included a Linksys WVBR0-25 wireless video bridge: this pipes video, audio and a user interface from your Directv Genie DVR over the air to up to eight Genie client boxes that are plugged into your TVs around the home.

The bridge sets up a private wireless network, and basically acts as a transparent coax cable to your television sets from the central Genie server. Lawshae homed in on the Linux-powered wireless bridge, and found it was running a web server. Incredibly, rather than hit a login form or similar, he found the built-in web server would cough up internal diagnostic information. What he saw was the Linksys kit running various setup scripts and log outputs; one of the scripts was building an MD5 hash out of his web browser's network IP address and user-agent string. By changing the browser's user-agent details – which is trivial – he was able to inject extra commands, which were run as the root user. Refreshing the page would interrupt the hash-generation code and instead run the injected commands – spitting out the user ID of the running script (root) and the Linux kernel

version. He bought one of the boxes on eBay, ripped them apart, and extracted the MXIC MX25L12845E 128Mb serial flash chip thatheld the firmware. In the code he confirmed the device was running a Lighttpd web server with no input sanitization in its custom scripts. So someone with access to the home network, say via an infected PC, would be able to leverage this vulnerability to install malware, spyware or a backdoor in the Linksys kit that would be virtually undetectable. The flaw would allow the device to be press- ganged into joining a botnet.

Now you'd think this wouldn’t be an issue for long. AT&T's a big company, as is Linksys, and they have a vested interest in protecting their customers and making sure that their kit isn't subverted. Not so it seems. "We reported this to them 181 days ago and gave them a couple of extensions," Dustin Childs, director of communications for the Zero Day Initiative, told The Register.