Security company finds vulnerability in Xfinity television remote controls

October 8 2020, by Bob Yirka

A team of researchers at GuardiCore Ltd., a cloud security company, has found a vulnerability in the remote controls Comcast provides its Xfinity user community. On their blog page, they relate how they were able to hijack the radio frequency (RF) communications emitted by the XR11 remote control device in a way that allowed them to listen to conversations taking place in the vicinity of the device.

Several years ago, cable TV and Internet provider Comcast began offering its Xfinity customers a new type of remote-control device that allowed voice commands to change channels and access other online services. The new remote, called the XR11, has been hugely successful for Comcast. According to the GuardiCore post, it is now the most popular remote in the country. In this new effort, researchers at GuardiCore found that it was possible to hijack the remote and to reprogram it for use as a secret recording device. They were able to mimic pressing the button that activated the listening device and then routed the human communications to a listening device some distance away. In so doing, they were able to use the remote as an illegal eavesdropping device.

On their blog post, the team at GuardiCore relates that they were looking for vulnerabilities in the set-top box that comes with Xfinity services, the device that normally communicates with the XR11 remote. After finding one vulnerability (which they promptly reported to Comcast), they turned their attention to the remote. They found that they were able to use an RF transceiver to install software onto the remote which then allowed them to manipulate the device itself. After some extensive reverse engineering, they discovered how the device worked and then reprogrammed it in ways they desired—one of which was turning on listening and broadcasting what it heard. The researchers found that the microphone on the device was of high enough quality that they could make out conversations by people up to 15 feet away from the remote.

GuardiCore reported their findings to Comcast before publishing their results, giving the company time to create a patch and send it out to their customers. Thus, the vulnerability no longer exists.

More information: WarezTheRemote: Turning Remotes Into Listening Devices: www.guardicore.com/2020/10/war … to-listening-devices