Bluetooth flaw in Linux kernel allows nearby hackers to execute code

16 October 2020, by Bob Yirka

Credit: Pixabay/CC0 Public Domain

Google engineer Andy Nguyen is reporting via a Twitter thread that a new security vulnerability has been found in Linux operating systems that run a Bluetooth software stack called BlueZ. Nguyen has named the vulnerability BleedingTooth and claims in his Twitter post that the vulnerability allows nearby hackers to conduct zero-click root-level code execution.

Linux is an operating system very similar to Unix—it became popular over a decade ago as a research and educational tool due to its open-source licensing and zero cost. In more recent years, it has been used to create dedicated applications—NASA uses it for many of its space applications, for example. It has also become popular for companies making Internet-of-Things (IoT) devices because it allows them to avoid royalty fees.

In this new effort, Nguyen has found a vulnerability that allows hackers within the range of a Bluetooth signal to gain root access to computers or devices running BlueZ. Notably, many IoT devices use BlueZ to allow users to communicate with their devices. Intel, a major backer of the group behind BlueZ, has announced that it is characterizing the vulnerability as a flaw that provides an escalation of privileges or the disclosure of information.

Because it is still a new discovery, little is known about the vulnerability—still, the team at BlueZ has released a patch for it and made it freely available. Also, Intel has issued an advisory on its web page, noting that the severity has been classified as high.

Despite the severity of the vulnerability, it is not considered to be something that the user community should worry about. A hacker would have to gain access to a building housing such a device or computer and have the necessary knowledge and equipment to take advantage of the situation. And there would also be the issue of motive—not many hackers are interested in taking over an IoT coffeepot sitting on someone's kitchen counter. As with many computer vulnerabilities, those most at risk are those who work with very sensitive or valuable information.