On 12 September 2017, Armis Labs announced eight zero day vulnerabilities in the Bluetooth protocol that could potentially impact billions of Bluetooth-enabled devices. Depending on the device, these vulnerabilities could result in remote code execution, man in the middle attacks, and information leakage. Their web site provides demonstrations of how vulnerabilities could be used to compromise Android, Windows and Linux based devices. The vulnerabilities include:

1. Linux kernel RCE vulnerability - CVE-2017-1000251
2. Linux Bluetooth stack (BlueZ) information Leak vulnerability - CVE-2017-1000250
3. Android information Leak vulnerability - CVE-2017-0785
4. Android RCE vulnerability #1 - CVE-2017-0781
5. Android RCE vulnerability #2 - CVE-2017-0782
Affected Devices

According to Armis, Bluetooth-enabled devices running Android, Linux, Windows, and pre-version 10 of iOS operating systems are impacted by at least one of the disclosed vulnerabilities. This covers a significant portion of connected devices globally.

The security researchers who uncovered BlueBorne estimate that 5.3 billion devices with Bluetooth capabilities are affected. However, certain conditions must exist before these vulnerabilities can be exploited:

- Bluetooth must be enabled
- The attacker must be within the Bluetooth-enabled device’s range (e.g. typically within 10 meters)
- The attack will vary per mobile platform (i.e. operating system), so having a single exploit that can target all devices is unlikely

What Does BlueBorne do?

The exploits used by Armis are proof of concept (POC) exploits that were demonstrated in a lab environment. The POC exploits have not been released, however the technical details of the exploits were disclosed in a technical white paper, so attackers may now be able to build exploits based on that information.

The Android demonstration showed an attacker taking remote control of an Android phone without the owner’s knowledge and activating the camera. The Windows demonstration showed a man-in-the-middle attack where the Windows user was redirected to a fake website and entered his e-mail, user id and password which were stolen by the attacker. The Linux demonstration showed an exploit used to eavesdrop on a Linux RCE smartwatch. The attacker then rebooted the device.

Armis did not demonstrate a worm that could spread from one device to another, but due to remote code execution, it might also be possible. However, as the Stagefright vulnerabilities proved, it is often very difficult in practice to come up with an exploit that will work across a wide range of software implementations. However, it is theoretically possible to build a worm that can spread to a large variety of Bluetooth devices, it is not likely.
What has been done?

Armis shared the details of the vulnerabilities and exploits with Google, Microsoft, Apple, Samsung and Linux in April 2017. They have worked since then to provide security updates to impacted systems prior to the coordinated disclosure on 12 September 2017.

- Microsoft made updates on 11 July 2017, and released one for CVE-2017-8628 as part of their September Patch on 12 September 2017.
- Apple has no vulnerability in its current versions. iOS 9.3.5 and AppleTV devices with version 7.2.2 (released in August and December 2016 respectively) and lower are affected, but those running iOS 10 are immune from CVE-2017-14315.
- Linux: Targeting updates for coordinated disclosure on or about 12 September 2017.

Recommendations

Most of the companies contacted by Armis in April have reacted by providing security updates to resolve the issue. Patching and keeping the OS updated help mitigate attacks that may leverage these vulnerabilities. Adopt best practices for mobile safety. Enforce patch management policies in enterprise environments. Users of Bluetooth devices should contact the device manufacturer to ensure that these updates have been applied to the products that they use. In the meantime, disable Bluetooth on devices when it is not being used.