BlueBorne Bluetooth Vulnerabilities

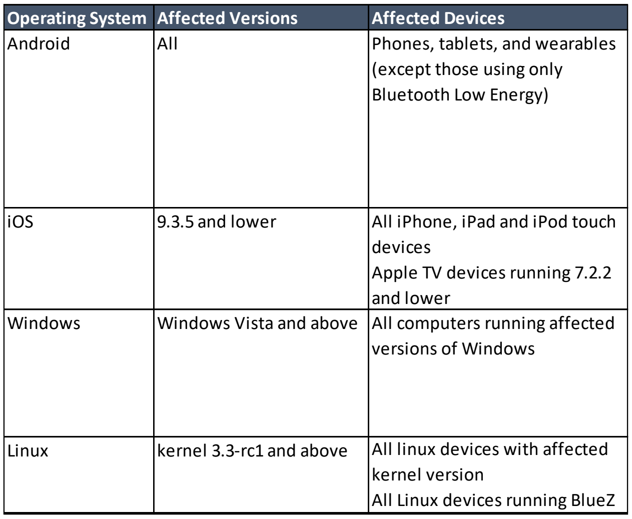
What is BlueBorne? BlueBorne is collection of several vulnerabilities in the Bluetooth protocol. As a result, a new attack vector affecting mobile, desktop and IoT operating systems, has been created. Through this attack a malicious entity can gain complete control of the target device, including access to any stored information. It was discovered by a US based IoT security lab, Armis.

What makes it dangerous? When combined the BlueBorne vulnerabilities could have a devastating impact on the target device. The following is a representative set of risks from this attack vector:

- Bluetooth is often overlooked while deploying network defense controls. This makes it as **easy entry point**, into the target machine, for a malicious entity.
- An attack leveraging BlueBorne vulnerabilities is capable of spreading from device to device. Thus, making it **highly infectious**.
- Bluetooth process has high privileges, by default, on most operating systems. Therefore, any attack exploiting the Bluetooth process could gain **full control** over the target device.
- Through this attack vector malicious hackers can also **penetrate into air gapped systems**.
- This attack **does not require any user intervention or preconditions**, except Bluetooth enabled, and is compatible with all software versions.
- This attack **does not requiring Bluetooth pairing**.

In simple terms, an unauthenticated, remote attacker may be able to obtain private information about the device or user, or execute arbitrary code on the device.

Which operating systems and devices are affected? BlueBorne vulnerabilities exist in major mobile, desktop and IoT operating systems. This includes Android, iOS, Windows and Linux.

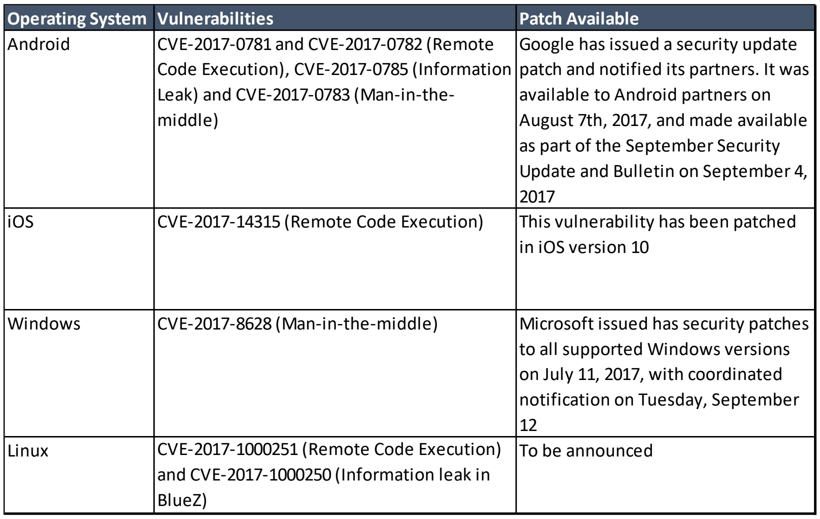


Operating System	Affected Versions	Affected Devices
Android	All	Phones, tablets, and wearables (except those using only Bluetooth Low Energy)
iOS	9.3.5 and lower	All iPhone, iPad and iPod touch devices Apple TV devices running 7.2.2 and lower
Windows	Windows Vista and above	All computers running affected versions of Windows
Linux	kernel 3.3-rc1 and above	All linux devices with affected kernel version All Linux devices running BlueZ

Demonstrations of this attack is available at (videos created by Armis)

- https://youtu.be/Az-l90RCns8 (Android)
- https://youtu.be/QrHbZPO9Rnc (Windows)
- https://youtu.be/U7mWeKhd_-A (Linux)

Which vulnerabilities are exploited and have they been patched? The following table lists the vulnerabilities and their patch status:



Operating System	Vulnerabilities	Patch Available
Android	CVE-2017-0781 and CVE-2017-0782 (Remote Code Execution), CVE-2017-0785 (Information Leak) and CVE-2017-0783 (Man-in-the-middle)	Google has issued a security update patch and notified its partners. It was available to Android partners on August 7th, 2017, and made available as part of the September Security Update and Bulletin on September 4, 2017
iOS	CVE-2017-14315 (Remote Code Execution)	This vulnerability has been patched in iOS version 10
Windows	CVE-2017-8628 (Man-in-the-middle)	Microsoft issued has security patches to all supported Windows versions on July 11, 2017, with coordinated notification on Tuesday, September 12
Linux	CVE-2017-1000251 (Remote Code Execution) and CVE-2017-1000250 (Information leak in BlueZ)	To be announced

What is its impact? It is estimated that BlueBlorne vulnerabilities affect more than 8.2 billion devices worldwide. These include all kinds of devices that are equipped with Bluetooth capabilities.

What prevention measures can be taken? Since most security solutions do not cater to Bluetooth capabilities there are hardly any controls available on this end other than deploying the patches that fix these vulnerabilities.

Organizations which have deployed a Mobile Device Management (MDM) solution can disable Bluetooth on devices running affected versions of mobile operating systems.

End-users should update their mobile devices to latest version of operating system released by the manufacturer. If an updated version is not available, they should exercise caution in using Bluetooth in public places and keep it disabled if not required.

References:

- https://www.armis.com/blueborne/
- http://www.androidpolice.com/2017/09/13/googles-september-security-patch-fixes-blueborne-bluetooth-vulnerability/
- https://www.kb.cert.org/vuls/id/240311