New Attack Vector "BlueBorne" Exposes Almost Every Connected Device

In September 2017, Armis reported a new attack vector endangering major mobile, desktop, and IoT operating systems, including Android, iOS, Windows, and Linux, and the devices using them. The new vector is dubbed "BlueBorne", as it spread through the air (airborne) and attacks devices via Bluetooth.

Armis has disclosed a total of nine related zero-day vulnerabilities, four of which are classified as critical. BlueBorne allows attackers to take control of devices, access corporate data and networks, penetrate secure "air-gapped" networks, and spread malware laterally to adjacent devices. Armis reported these vulnerabilities to Google, Microsoft, Apple, Linux, and Amazon, and worked with them as patches are being identified and released as part of a responsible disclosure process. BlueBorne impacted more than 5.3 billion devices, many of which are used in the workplace. More than 1.2 billion were identified as "forever day," and not patchable.

What Is BlueBorne?

BlueBorne is an attack vector by which hackers can leverage Bluetooth connections to penetrate and take complete control over targeted devices. BlueBorne affects ordinary computers, mobile phones, and the expanding realm of IoT devices. The attack does not require the targeted device to be paired to the attacker's device, or even to be set on discoverable mode.

A Comprehensive and Severe Threat

The BlueBorne attack vector requires no user interaction, is compatible to all software versions, and does not require any preconditions or configurations aside of the Bluetooth being active. Unlike the common misconception, Bluetooth enabled devices are constantly searching for incoming connections from

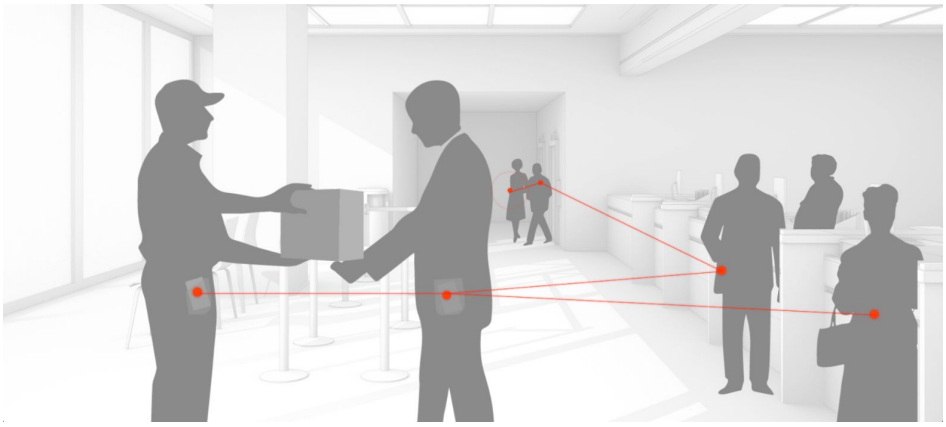
BlueBorne requires no user interaction, nor does it require the devices to "pair." Bluetooth just has to be on for a connection to be made.

any devices, and not only those they have been paired with. This means a Bluetooth connection can be established without pairing the devices at all. This makes BlueBorne one of the broadest potential attacks found in recent years, and allows an attacker to strike completely undetected.

BlueBorne Explained

How the Attack Vector Works

The BlueBorne attack vector has several stages. First, the attacker locates active Bluetooth connections around him or her. Devices can be identified even if they are not set to “discoverable” mode.



One infected device can spread to other devices or systems directly via Bluetooth without user interaction.

Next, the attacker obtains the device’s MAC address, which is a unique identifier of that specific device. By probing the device, the attacker can determine which operating system his victim is using, and adjust his exploit accordingly. The attacker will then exploit a vulnerability in the implementation of the Bluetooth protocol in the relevant platform and gain the access he needs to act on his malicious objective.

At this stage, the attacker can choose to create a Man-in-The-Middle attack and control the device’s communication, or take full control over the device and use it for a wide array of cybercriminal purposes.

At Black Hat Europe 2018, Armis demonstrated the world’s first Bluetooth worm live on stage. This included the first non-physical remote code execution on an Amazon Echo.

Personal Assistants like Amazon Echo and Google Home were vulnerable to BlueBorne

What Devices Are Affected?

Android

All Android phones, tablets, and wearables (except those using only Bluetooth Low Energy) of all versions are affected by four vulnerabilities found in the Android operating system, two of which allow remote code execution (CVE-2017-0781 and CVE-2017-0782), one results in information leak (CVE-2017-0785) and the last allows an attacker to perform a Man-in-The-Middle attack (CVE-2017-0783).

Google has issued a security update as part of the September Security Update and Bulletin on September 4, 2017.

Windows

All Windows computers since Windows Vista are affected by the "Bluetooth Pineapple" vulnerability which allows an attacker to perform a Man-in-The-Middle attack (CVE-2017-8628).

Microsoft issued has security patches to all supported Windows versions on July 11, 2017, and recommend that Windows users should check with the Microsoft Patch Tuesday information on September 12, 2017 for the latest information.

Linux

Linux is the underlying operating system for a wide range of devices. The most commercial, and consumer-oriented platform based on Linux is the Tizen OS.

- All Linux devices running BlueZ are affected by the information leak vulnerability (CVE-2017-1000250).
- All Linux devices from version 2.6.32 (released in July 2009) until version 4.14 are affected by the remote code execution vulnerability (CVE-2017-1000251 and CVE-2017-1000410).

Patches to Linux vulnerabilities have been pushed to the upstream projects. The information leak vulnerability was patched, and the remote code execution was patched here. Linux distributions have started to push updates as well, please look for specific updates made by your distribution.

iOS

All iPhone, iPad and iPod touch devices with iOS 9.3.5 and lower, and Apple TV devices with version 7.2.2 and lower are affected by the remote code execution vulnerability (CVE-2017-14315). This vulnerability was already mitigated by Apple in iOS 10, so no new

patch is needed to mitigate it. We recommend you upgrade to the latest iOS or tvOS available.

If you are concerned that your device may not be patched, we recommend disabling Bluetooth, and minimizing its use until you can confirm a patch is issued and installed on your device.

For More Information

For more information, included video demonstrations and a complete technical white paper, please visit **armis.com/blueborne**.

About Armis
Armis eliminates the IoT security blind spot, protecting enterprises from the threat of unmanaged or rogue devices. Fortune 1000 customers trust Armis' agentless IoT security platform to discover and analyze any device, protecting their business critical information and systems. Armis is a privately held company and headquartered in Palo Alto, California.
armis.com