Bluetooth BlueBorne Vulnerabilities

A new attack vector exposes almost every connected device.

General Overview

A tech company, Armis, revealed 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 spreads through the air (airborne) and attacks devices via Bluetooth. Armis has also disclosed eight 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 the responsible actors (Google, Samsung, Galaxy, Apple, etc.), and is working with them as patches are being identified and released.

What Is BlueBorne and how does it work?

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. Armis Labs has identified eight zero-day vulnerabilities so far, which indicate the existence and potential of the attack vector. Armis believes many more vulnerabilities await discovery in the various platforms using Bluetooth. These vulnerabilities are fully operational, and can be successfully exploited, as demonstrated in Armis' research. The BlueBorne attack vector can be used to conduct a large range of offenses, including remote code execution as well as Man-in-The-Middle attacks.

What Is The Risk?

The BlueBorne attack vector has several qualities which can have a devastating effect when combined. By spreading through the air, BlueBorne targets the weakest spot in the networks' defense – and the only one that no security measure protects. Spreading from device to device through the air also makes BlueBorne highly infectious. Moreover, since the Bluetooth process has high privileges on all operating systems, exploiting it provides virtually full control over the device.

How Wide Is The Threat?

The BlueBorne attack vector can potentially affect all devices with Bluetooth capabilities, estimated at over 8.2 billion devices today. Bluetooth is the leading and most widespread protocol for short-range communications, and is used by devices of all kinds, from regular computers and mobile devices to IoT devices such as TVs, watches, cars, and even medical appliances. The latest published reports show more than 2 billion Android,

2 billion Windows, and 1 billion Apple devices in use. Gartner reports that there are 8 billions connected or IoT devices in the world today, many of which have Bluetooth.

Unlike traditional malware or attacks, the user does not have to click on a link or download a questionable file. No action by the user is necessary to enable the attack other than turn on the Bluetooth in your device

This is 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. This is important point to note. Unlike the common misconception, Bluetooth enabled devices are constantly searching for incoming connections from any devices, and not only those with which they have been paired. 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.

Affected Devices

The vulnerabilities disclosed by Armis affect all devices running on Android, Linux, Windows, and pre-version 10 of iOS operating systems, regardless of the Bluetooth version in use. This means almost every computer, mobile device, smart TV or other IoT device running on one of these operating systems is endangered by at least one of the eight vulnerabilities. This covers a significant portion of all connected devices globally.

What Devices Are Affected?

Android
Examples of impacted devices:
•Google Pixel
•Samsung Galaxy
•Samsung Galaxy Tab
•LG Watch Sport
•Pumpkin Car Audio System

Google has issued a patch and notified its partners. It will be available for:
•Nougat (7.0)
•Marshmallow (6.0)

Note to Android users: To check if your device is at risk or whether the devices around you are at risk, download the Armis BlueBorne Scanner App on Google Play (link not provided)

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.

Linux
Linux is the underlying operating system for a wide range of devices. Examples of impacted devices with Linux:
•Samsung Gear S3 (Smartwatch)
•Samsung Smart TVs
•Samsung Family Hub (Smart refrigerator)

Apple iOS system
All iPhone, iPad and iPod touch devices with iOS 9.3.5 and lower, and AppleTV devices with version 7.2.2 and lower are affected by the remote code execution vulnerability. 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.

What You Should Do
Now that we know the issues and risks, what do we do? Armis reached out to Google, Samsung, Apple, Linux, etc. to ensure a safe, secure, and coordinated response to the vulnerabilities identified. However, in the meantime, if you are concerned that your device may not be patched, **we recommend disabling Bluetooth (turning it off), and minimizing its use (using it only when needed and turning it off thereafter) until you can confirm a patch is issued and installed on your device.**