BlueBorne - Impact Analysis

Kees de Jong
Kotaiba Alachkar
Adrien Raulot
Shahrukh Zaidi

Table of contents

Abstract

Bluetooth has found its way on almost any modern device ranging from desktops to smart watches or even refrigerators. Recently a set of eight zero-day vulnerabilities were discovered of which four were classified as critical. These vulnerabilities are dubbed as “BlueBorne”. What makes these vulnerabilities critical is that it spreads through the air and can take full control of the devices without the victim being aware of it. If a device is infected, it can spread to other vulnerable devices within its range. Merely having Bluetooth enabled is enough to become a target.

Introduction

Recently, Armis Labs 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 spread 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, and is working with them as patches are being identified and released. A whitepaper has also been released describing the technical details of these vulnerabilities (source).

Scope

The aim of this project is to analyze the impact of the BlueBorne vulnerabilities. The main research question we want to answer is the following:

What is the potential impact of the BlueBorne vulnerabilities?

To answer this question, we will first review which devices are impacted (type, version, etc). Then, some devices are already fixed, some will be soon but also some devices won’t get to be (easily) fixed e.g. old smart TV’s and Android phones. It would be interesting to find ways to protect these devices nonetheless. And if we can’t find ways to protect these products, we can at least point out what didn’t work so that future work can continue to look for better solutions. On top of that, we found the spreading aspect of BlueBorne interesting and will investigate on how creating a worm using the BlueBorne vulnerabilities could be possible.

The main purposes of this research are to have a better overview on the worldwide impact of the BlueBorne vulnerabilities. We think it would also be interesting to look at the impact within the University of Amsterdam campus and see, a couple of weeks after we first heard about BlueBorne, what have been done to mitigate these attacks and if people at the University have their devices protected against them.

Tooling

- Raspberry Pi 3 (with vulnerable BlueZ and kernel to test and troubleshoot)
- Smartphone with an old Android version (and hence vulnerable to BlueBorne)
- BlueBorne scanner (to collect data of potential impact at the university itself)
- bluetoothctl
- Ubertooth hardware (GitHub)
- Wireshark
- OpenVAS (if it includes the functionality to test this specific vulnerability)
- IRC channels (white/grey hat community can be a great source for information)
- Bluez-hcidump (output after pairing with a device, which was done by *bluetoothctl*)

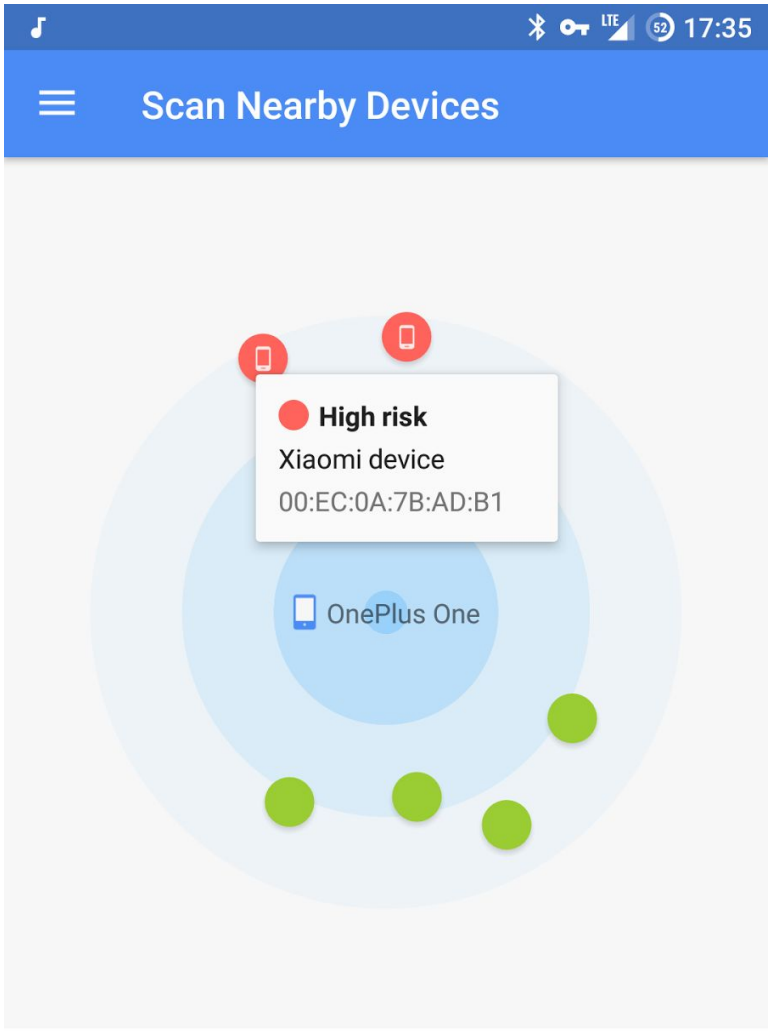
Videos

Android Take Over Demo
Linux Smartwatch Take Over Demo
Windows MiTM Demo

Other resources

Bluetooth protocol stack log for Linux (release 5.47 contains all the fixes for BlueBorne)

Presumably valid code to test BlueBorne (code review required):
~~Blueborne-scanner~~ (not working/incomplete, maybe will be improved in the coming days)
https://github.com/mailinneberg/BlueBorne / https://github.com/johndpope/blueborne



Devices Risk Results

Tap on any dot above for more information.

Get Full IoT Security Assessment

[BlueBorne Vulnerability Scanner by Armis]