CERT-EU Security Advisory 2017-018

BlueBorne Attack against Bluetooth

September 14, 2017 — v1.1

History:

- *13/09/2017 — v1.0 – Initial publication*
- *14/09/2017 — v1.1 – Corrected some typos*

Summary

A new attack vector endangering major mobile, desktop, and IoT operating systems and the devices using them – including Android, iOS, Windows, and Linux – has been revealed by Armis Labs [1]. The new attack 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, and is working with them as patches are being identified and released [1].

Technical Details

The full description of the vulnerabilities and security flaws can be found in the whitepaper [2].

The attack is notable for its unusual reach and effectiveness. Essentially any Android, Linux, or Windows device that has not been recently patched and has Bluetooth turned on can be compromised by an attacking device in the Bluetooth range (around 10 meters). The attack does not require device users to click on any links, connect to a rogue Bluetooth device, or take any other action. The exploit process is generally very fast, requiring no more than 10 seconds to complete, and it works even when the targeted device is already connected to another Bluetooth-enabled device [3].

Products Affected

- Android phones, tablets, and wearables – except those using only Bluetooth Low Energy (CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, and CVE-2017-0785).
- Linux devices running BlueZ[1] version `5.46` and earlier are affected by the information leak vulnerability (CVE-2017-1000250).

[1] Linux Bluetooth protocol stack – http://www.bluez.org

- Linux devices from kernel version `3.3-rc1` (released in October 2011) up to and including kernel version `4.13.1` are affected by the remote code execution vulnerability (CVE-2017-1000251).
- Microsoft 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).
- Apple iOS: 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.

Recommendations

- Apply patches for the above mentioned vulnerabilities provided by the respective vendors and OS maintainers.
- As workaround – consider entirely disabling Bluetooth.

References

[1] https://www.armis.com/blueborne/

[2] http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf

[3] https://arstechnica.com/information-technology/2017/09/bluetooth-bugs-open-billions-of-devices-to-attacks-no-clicking-required/