

Ikt. sz.: 30700-0/4871-13/2017

TLP: WHITE
Szabadon terjeszthető!

Riasztás

BlueBorne, Bluetooth eszközök sérülékenységei (2017.09.13.)

Tisztelt Ügyfelünk!

A Kormányzati Eseménykezelő Központ riasztást ad ki **Bluetooth eszközök sérülékenységei** miatt.

Az Armis biztonsági kutatói nyolc új sebezhetőséget fedeztek fel a Bluetooth implementációkban, amelyeket együttesen **BlueBorne**-nek neveztek el. Ez a legsúlyosabb Bluetooth sérülékenység, amelyet eddig azonosítottak.

A nyolc biztonsági hiba közül három kritikus besorolású. Ezek lehetővé teszik a támadók számára, hogy átvegyék az eszközök irányítását és rosszindulatú kódokat futassanak le, vagy a közbeékelődéses (Man-in-the-Middle) támadások hajtsanak végre. A Bluetooth-ban talált korábbi hibák elsősorban protokoll szinten voltak. A BlueBorne hibái viszont a végrehajtási szinten vannak, megkerülve ezzel különböző hitelesítési mechanizmusokat.

A kutatók szerint a sérülékenységek észrevehetetlenek és megállíthatatlanok a hagyományos biztonsági megoldásokkal. **Nincs szükség felhasználói interakcióra** a támadónak a BlueBorne hibáinak használatához, és a támadónak sem kell párosítania eszközét a célkészülékkel.

A hiba több mint **5,3 milliárd eszközt érint**. Szinte minden Android, iOS, Microsoft és Linux Bluetooth implementáció sérülékeny lehet. Így szinte minden Bluetooth-t használó eszköztípust érintenek, az okostelefonokat, a laptopokat, valamint az IoT eszközöket és az intelligens autókat.

Az Armis bejelentette a biztonsági hibákat a legfontosabb hardver- és szoftvergyártóknak úgymint, Apple, Google, Microsoft és a Linux közösség számára. A biztonsági javítások vélhetően az elkövetkező napokban és hetekben elérhetőek lesznek, azonban **nem minden eszköz kap javítást**. Tipikusan azok az eszközök, melyeknek élettartama lejárt és a gyártók már nem frissítik a Bluetooth-kompatibilis készülékek mintegy 40%-a, ami több mint két milliárd tartósan sérülékeny készüléket jelent.

Ki érintett?

Az összes Android telefon, tablet és hordozható készülék minden változata sérülékeny. Kivéve a Bluetooth Low Energy technológiát használó Android eszközöket. A Google szeptemberi Android biztonsági frissítéseivel javította a hibákat.

Microsoft esetében a Windows Vista óta az összes operációs rendszer, összes változata. A Microsoft szerint a BlueBorne nem befolyásolja a Windows telefonokat. A Microsoft júliusban megjelentette a javításokat, de csak a szeptemberi frissítésekkor publikáltak részleteket a javított sérülékenységről.

A BlueZ-t futtató összes Linux-rendszert információs szivárgás érinti, míg a 3.3-rc1 (2011. októberében kiadott) Linux-eszközöket a távoli kód futtatás által okozott hibák érintik.

Az iPhone, iPad és iPod touch készülékek iOS 9.3.5 és régebbi verziói, az AppleTV 7.2.2-es és régebbi verziókkal rendelkező eszközök. A probléma javításra került az iOS 10-ben.

A **GovCERT javasolja Bluetooth letiltását**, ameddig meg nem győződött róla, hogy az eszköz nem sérülékeny. Android felhasználók számára a Google Play Store-ból letölthető **BlueBorne Android App**, amivel könnyen ellenőrizhető az eszköz sérülékenysége.

Tájékoztató:

<http://tech.cert-hungary.hu/vulnerabilities/CH-14221>

<http://tech.cert-hungary.hu/vulnerabilities/CH-14225>

További információ:

<https://www.bleepingcomputer.com/news/security/blueborne-vulnerabilities-impact-over-5-billion-bluetooth-enabled-devices/>

Kormányzati Eseménykezelő Központ
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu