BlueBorne - provala kroz Bluetooth vezu

Poprilično neugodan problem pojavio se ovih dana: otkriven je niz propusta kroz koje napadači mogu ostvariti nadzor nad uređajem koji koristi Bluetooth vezu: CVE-2017-1000251, CVE-2017-1000250, CVE-2017-0785, CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, CVE-2017-8628, CVE-2017-14315.

Posebice neugodna je činjenica da napadač, da bi ostvario uspješan napad, ne treba biti uparen sa uređajem kojeg napada, već je dovoljno da se nađe u njegovoj blizini: napad je moguće ostvariti čim se napadač nađe u dometu BT signala.

Rezultat uspješnog napada dobivanje je pristupa napadnutom uređaju sa povišenim privilegijama, nakon čega je moguće instalirati maliciozni payload. Dapače, kako autori tvrde, ovaj napad posebno je opasan jer se može "širiti zrakom", odnosno jedan zaraženi uređaj može aktivno zaraziti sve druge uređaje u svojoj blizini.

Na napad su osjetljivi uređaji koji koriste Linux OS, Windows OS i Android.

Kako je već i red, vjerojatno već imate instalirane sigurnosne zakrpe za Linux i Windows računala, no puno veći problem ovdje je - Android. I to ne zbog sebe (Google je također već izbacio sigurnosne zakrpe), nego zbog starog običaja proizvođača uređaja koji koriste Android da svoje proizvode nakon nekog vremena praktički zaborave i za njih više nikad ne ponude niti najnužnije sigurnosne zakrpe, a kamoli novu verziju OS-a.

Ta nas činjenica uvodi u najrazorniji problem BlueBorne napada: milijuni i milijuni uređaja, od pametnih telefona do pametnih televizora i IoT gadgeterije, svi redom osjetljivi na napad koji je moguće izvesti bez fizičke prisutnosti i, uz dobru opremu, sa sigurne udaljenosti od žrtve. Jednom provaljen, mnogi takav uređaj ostat će provaljen. A ako vam paranoja još nije proradila, zamislite što se sve može učiniti sa pametnim televizorom koji ima ugrađenu kameru i mikrofon.

Svakako, još jedan razlog više da dobro razmislite o izoliranju privatne opreme korisnika u zasebnu mrežu: zaražene telefone teško ćete otkriti, a još teže očistiti. Teoretski, svaki od tih uređaja koji neće dobiti sigurnosnu zakrpu šetajući je vektor zaraze izvan vaše kontrole.

Za one koji žele znati više, autori su pripremili simpatičan whitepaper na adresi http://go.armis.com/blueborne-technical-paper [1].

pon, 2017-09-18 15:27 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [2]
Vote: 0

No votes yet

story_tag: bluetooth [3]
BlueBorne [4]

Source URL: https://sysportal.carnet.hr/node/1760

Links
[1] http://go.armis.com/blueborne-technical-paper
[2] https://sysportal.carnet.hr/taxonomy/term/14
[3] https://sysportal.carnet.hr/taxonomy/term/137
[4] https://sysportal.carnet.hr/taxonomy/term/138