Negyvenéves parancskészlet miatt egy töltővel feltörhetők az androidos telefonok

Egy 1981 óta létező utasításkészlet miatt hozzá lehet férni egy sor androidos okostelefon és tablet adataihoz. A veszély nem csak elméleti, és az IoT eszközökben is problémát okozhat.

Több millió okostelefont és tabletet veszélyeztet egy olyan sérülékenység, amit a közelmúltban azonosított egy kutatócsapat. A sérülékenység kihasználásával akár a teljes irányítást meg lehet szerezni a megtámadott rendszer fölött. A legnagyobb gyártók, többek között a Asus, a Google, a HTC, a Huawei, a Lenovo, az LG, a Motorola, a Samsung, a Sony és a ZTE készülékei is veszélyben vannak – írja a ThreatPost.

Egy ősrégi parancskészlet a bűnös

A sérülékenységre egy kutatási projekt derített fényt, melyben a Floidai Egyetem, a New York-i Állami Egyetemhez tartozó Stony Brook Kutatóegyetem és a Samsung amerikai kutatóközpontjának munkatársai vizsgálták az ún. AT-parancsok nyújtotta támadási felületeket.

Az AT (ATtention) parancsok az ún. Hayes parancskészlet egy csoportjának gyűjtőneve. Ezt a parancskészletet *Dennis Hayes,* a modemgyártó Hayes Microcomputer Products alapítója, fejlesztette ki 1981-ben modemjeihez. Ezekkel a parancsokkal lehetett létrehozni a modemes kapcsolatot, azaz tárcsázni, felépíteni a kapcsolatot vagy a kapcsolat paramétereit módosítani. Bár azóta sok minden változott, a parancskészlet egy részét mind a mai napig használják – például a mobiltelefonok is.

Bár a Hayes parancskészlet kiadása óta nagyon sokat fejlődött a kommunikáció, a parancskészletet a fejlesztők adottnak vették, és nem is nagyon foglalkoztak vele. Érvényesült a régi – és gyakran rossz eredményre vezető elv –, hogy ami működik, ne akarjuk megjavítani. A kutatók kiderítették, hogy a korábbi szórványos támadások ezért is következhettek be: a készülékgyártók ugyanis nem építettek megfelelő védelmi mechanizmusokat az AT-parancsok köré.

A parancskészlet nagyon rugalmas. Van ugyan egy olyan alap, amit minden készülékeknek támogatnia kell, de ez szabadon bővíthető, és a gyártók lelkesen bővítik is. Az AT-parancsokat sok esetben amolyan univerzális interfészként használják az operációs rendszer és az alacsonyabb szintű összetevők, például az alapsávi modem között, és sok funkciót ezekkel oldanak meg – sokszor dokumentálatlan módon. A kutatók éppen ezért aprólékosan végignéztek több mint kétezer androidos firmware-t. Így végül több mint 3500 különféle AT-parancsot találtak.

A kutatás egyébként még csak az első fázisában tart. Eddig azt vizsgálták, hogyan lehet a parancsokat kiaknázni az USB porton keresztül – a wifis és a bluetooth-os kapcsolat vizsgálata még folyik. Bár a feltárt kockázatok eszközönként eltérőek voltak, szinte mindegyik kellően súlyos volt ahhoz, hogy lényegében védtelenné tegye a készüléket egy esetleges támadással szemben.

Ezekre lehet használni a védtelen AT-parancsokat

A kutatás során nem csak a potenciális sérülékenységeket tárták fel, hanem arra is készítettek proof of conceptet, hogy azokat hogyan és mire lehet kihasználni. Lehet módosítani a firmware-t,

meg lehet kerülni a rendszer védelmi mechanizmusait, fel lehet oldani a képernyőzárat, adatokat lehet ellopni a készülékről, különféle műveleteket lehet végrehajtani a rendszerben. A kutatók sok készüléknél találtak olyan nem dokumentált AT-parancsokat is, amelyek segítségével a támadó teljes mértékben átveheti az irányítást az adott készülék felett.

Emellett sikerült kiolvasni az IMEI-azonosítót, az akkumulátor töltöttségi szintjét, a telefon sorozatszámát, a gyártót, a szoftververziót és a SIM-kártya adatait is.

A legnagyobb veszélynek azok a készülékek vannak kitéve, melyek zárolt képernyő esetén is reagálnak az AT-parancsokra. Szerencsére a vizsgált rendszerek többségénél ez nincs így, és csak akkor vannak veszélyben, ha a felhasználó engedélyezi az USB hibakeresés funkciót. Tegyük hozzá gyorsan, ez azért nem kézenfekvő, hiszen ez a funkció alapból nem érhető el. Használatához be kell lépni a fejlesztői módba, amit csak a legelszántabb felhasználók szoktak megtenni. Emellett a telefonhoz fizikailag is hozzá kell férni, hogy az USB proton keresztül lehessen vele kommunikálni.

Ugyanakkor az is bebizonyosodott, hogy a fejlesztői módban és az USB hibakeresés funkciót bekapcsolva használt készülékeket akár egy reptéri töltőállomáson is simán feltörhetik, mert a töltőn keresztül nem csak áram, hanem minimális kód is bejuttatható a rendszerbe.

A kutatók felfedezéseikről értesítették az érintett gyártókat. A munkát ki akarják terjeszteni az iPhone-okra, valamint az IoT eszközökre is, melyek szintén használnak AT-parancsokat.

Ez a cikk független szerkesztőségi tartalom, mely a T-Systems Magyarország támogatásával készült. Részletek: https://bitport.hu/impresszum#szponzoracioChromeHTML\Shell\Open\Command

Forrás: **https://bitport.hu/uj-veszelyforrast-talaltak-az-androidos-telefonokban-az-iot-eszkozok-sincsenek-biztonsagban**

Válogatta: Fonyó Istvánné