CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 19.05.2020 г.

Нова Bluetooth уязвимост излага милиарди устройства на опасност

19 май 2020 г.

Експерти по сигурността разкриха уязвимост в сигурността на Bluetooth, която потенциално би могла да позволи на нападателя отдалечено да излъже сдвоено устройство, излагайки на опасност над милиард съвременни устройства.

Атаките, наречени Bluetooth Impersonation AttackS или BIAS, се отнасят до Bluetooth Classic, който поддържа Basic Rate (BR) и Enhanced Data Rate (EDR) за безжичен трансфер на данни между устройствата.

Bluetooth съдържа уязвимости, които позволяват да се извършат атаки по време на установяване на сигурна връзка. Такива уязвимости включват липсата на задължително взаимно удостоверяване, прекомерно разрешено превключване на ролите и понижаване сигурността на процедурата за удостоверяване.

Като се има предвид широкото въздействие на уязвимостта, изследователите отговорно разкриват откритията пред Bluetooth групата за специални интереси (SIG) - организацията, която наблюдава развитието на стандартите за Bluetooth през декември 2019 г.

Bluetooth SIG групата призна недостатъка, добавяйки, че е направила промени, за да разреши уязвимостта. Тези промени ще бъдат въведени в бъдеща ревизия на спецификациите.

BIAS атаката

За да бъде успешна BIAS атаката, атакуващото устройство трябва да бъде в обхвата на безжичната мрежа на уязвимо Bluetooth устройство, което преди това е установило BR / EDR връзка с друго Bluetooth устройство, чийто адрес е известен на нападателя.

Недостатъкът произтича от това как две сдвоени преди това устройства се справят с дългосрочния ключ, известен също като ключ за връзка, който се използва за взаимна идентификация на устройствата и активиране на защитена връзка между тях.

Ключът за връзка гарантира, че потребителите не трябва да сдвояват своите устройства всеки път, когато се случи пренос на данни между, например, безжична слушалка и телефон или между два лаптопа.

Тогава нападателят може да използва грешката, за да поиска връзка с уязвимото устройство, като подправи Bluetooth адреса на другия, като по този начин подправя самоличността и получава пълен достъп до друго устройство, без всъщност да притежава ключа за дългосрочно сдвояване, който е бил използван за установяване на връзка.

Казано по различен начин, атаката позволява на нападател да представи себе си за устройство, сдвоено преди това с целевото устройство.

Нещо повече, BIAS може да се комбинира с други атаки, включително атаката KNOB (Key Negotiation of Bluetooth), която се случва, когато трета страна принуди две или повече жертви да се споразумеят за ключ за криптиране с намалена сигурност, като по този начин позволява на атакуващия да извърши атака по метода на грубата сила.

Устройствата, които не са актуализирани от декември 2019 г., са засегнати

Изследователи са тествали атаката срещу 30 устройства, включително смартфони, таблети, лаптопи, слушалки и компютри като Raspberry Pi. Установено е, че всички устройства са уязвими към BIAS атаки.

От Bluetooth SIG актуализират спецификацията на Bluetooth Core, за да избегнат понижаване на сигурните връзки, което позволява на атакуващия да инициира превключвател на роли от типа master-slave, за да се постави в главната роля и да стане инициатор на удостоверяване.

Как да се предпазим от атаката

В допълнение към призива на компаниите да бъдат приложени необходимите корекции в Bluetooth, на потребителите се препоръчва да инсталират най-новите актуализации от производителите на устройството и на операционната система.

Атаките BIAS са първите проблеми, свързани с процедурите за удостоверяване на сигурността при установяване на защитена връзка с Bluetooth, с превключватели на роли и с понижаване на сигурността на връзките. BIAS атаките са скрити, тъй като установяването на защитена Bluetooth връзка не изисква взаимодействие с потребителя.

За повече информация:

https://thehackernews.com/2020/05/hacking-bluetooth-vulnerability.html