A new security flaw allowed to impersonate Bluetooth peripherals

A new security hole of Bluetooth peripherals could be exploited to connect to malicious devices.

A team of researchers has revealed a new vulnerability that could allow an attacker to deceive modern Bluetooth-enabled server devices to pair with a malicious device masquerading as a trusted device. . The security flaw has been named Bluetooth Impersonation Attacks (BIAS), and it can affect a wide range of Bluetooth-enabled devices, including iPhones, iPads and Macs.
Basically, BIAS attacks exploit vulnerabilities in the way Bluetooth devices handle long-term connections. When two Bluetooth devices are paired, there will be a connection code called a 'link key' automatically, which will allow them to connect again in the future without having to perform the pairing procedure again. concatenated as the original. The group of scholars at the Polytechnique Federale de Lausanne in Switzerland found that they could forge the Bluetooth address of a previously paired device to complete the authentication process without knowing this 'link key'.

BIAS attack via Bluetooth has been discovered

When this vulnerability is combined with other security exploiting features such as Key Negotiation of Bluetooth (KNOB), an attacker can easily authenticate with devices running in Secure Authentication mode. When the BIAS attack succeeds, an attack device can be used to perform other security exploits, including accessing data sent via Bluetooth or even controlling the functions that a device has. was paired previously had.

What devices can be attacked by BIAS?

This vulnerability only affects the Bluetooth Basic Rate / Enhanced Data Rate of the Bluetooth connection, also known as Bluetooth Classic. But still caused relatively new Apple devices, including iPhone 8 and above, 2017 MacBook devices and above, and 2018 or newer iPad models.
In order to perform the attack, the bad guy will need to be in the Bluetooth range of the vulnerable device and need to know the Bluetooth address of the previously paired device. For a skilled attacker, finding these Bluetooth addresses is not difficult, even if they are random. To minimize the possibility of being hacked, turn off Bluetooth when you are not using or forget all devices you have previously paired.
The researchers alerted the Bluetooth Special Interest Group (SIG), and the team updated the Bluetooth Core Specification to minimize the flaw. It's likely that manufacturers like Apple and Samsung will roll out firmware or software patches in the near future.