Health-ISAC Vulnerability Bulletin: Bluetooth Impersonation Attacks (BIAS) Allow Impersonation on Thousands of Devices

Vulnerability Bulletins | TLP: WHITE | Alert Id : c95e8b94 | May 20, 2020, 03:55 PM

Summary:

Bluetooth (BR/EDR) is a pervasive technology for wireless communication used by over a billion devices across the globe. The Bluetooth standard includes a legacy authentication procedure and a secure authentication procedure, allowing devices to authenticate to each other using a long-term key for a consistent connection over a longer period. Those procedures are used during pairing and secure connection establishment to prevent impersonation attacks.

Security researchers have shown that the current Bluetooth specification contains vulnerabilities enabling impersonation attacks during secure connection establishment. Such vulnerabilities include the lack of mandatory mutual authentication, overly permissive role switching, and authentication procedure downgrades. Researchers utilized the vulnerabilities in attacks known as Bluetooth Impersonation AttackS (BIAS).

The attacks are standard compliant and are therefore effective against any standard compliant Bluetooth device regardless of the Bluetooth version, the security mode (e.g., Secure Connections), the device manufacturer, and the implementation details. The researchers successfully conducted the attack against 31 Bluetooth devices (28 unique Bluetooth chips) from major hardware and software vendors, implementing all the major Bluetooth versions, including Apple, Qualcomm, Intel, Cypress, Broadcom, Samsung, and CSR.

At this time, there have been no recorded instances of the vulnerability being exploited in the wild. The research team behind the vulnerability discovery recently published their research paper and provided their first public presentation of the issue on May 18, 2020. After the presentation was made public on Monday, there have been only a few media stories covering the issue as of this publication time.

Analysis:

The attacker's primary goal is to establish a secure Bluetooth connection with two users attempting to connect, while pretending to be the other user, intercepting the data shared between them. This can be accomplished by impersonating both users at the same time, utilizing a deprecated and insecure authentication method.

For the attack to successfully execute, the attacker must be capable of eavesdropping, decoding and manipulating unencrypted packets, as well as jamming the Bluetooth spectrum. The attacker needs to know the public information about each user, such as their Bluetooth names, Bluetooth addresses, protocol version numbers, and capabilities.

When two devices initiate procedures for a secured Bluetooth connection, the attacker can collect the device details by eavesdropping on their initial communication, as the data is not yet encrypted. If the secure connection between the users is already established, the attacker must jam the Bluetooth spectrum to force the users to automatically disconnect and re-establish the secure connection that an attacker can eavesdrop.

Users initially pair once to agree upon a long-term key, and then authenticate that they will use the long-term key upon secure connection establishment using either legacy secure connection or the more modern, standard secure connection method. The type of communication method is decided by the firmware version and device capabilities between the two devices.

Attackers can spoof the Bluetooth address of either victim but cannot prove the ownership or possession of the secured long-term key. This is the fundamental assumption behind Bluetooth's authentication guarantees, and this assumption should protect against impersonation attacks.

Bluetooth Impersonation Attacks can occur for several reasons:

- The Bluetooth secure connection establishment procedure is not integrity protected, despite the legitimate devices already sharing a long-term key. The lack of integrity protection allows an attacker to modify the capabilities of the impersonated victim, including secure connections support.
- Bluetooth additionally does not enforce the usage of secure connections between pairing and secure connection establishment. Hence, two devices who paired using secure connections can use the legacy secure connections method to reestablish subsequent secure connections. The attacker exploits this to downgrade a secure connection establishment to legacy secure connections in order to use the more vulnerable procedure.

To conduct the BIAS attacks,
attackers target the legacy secure connection authentication procedure during the initial secure connectio n establishment. Both procedures authenticate the long-term key using a challenge-response protocol, and the procedure selection depends on victims' supported features.

Attackers can downgrade the modern secure connection method to the
more vulnerable legacy authentication procedure, which remains the preferred attack vector.
Secure Connections uses stronger cryptographic primitives than legacy security connections and is considered the most secure way to pair and establish secure connections, making legacy more desirable to exploit for malicious actors.

The legacy authentication procedure provides unilateral authentication for both devices. When two users are pairing, such a procedure is used to achieve mutual authentication for the slave-master relationship between devices. A central issue and primary exploit in BIAS attacks is that the Bluetooth standard does not require the use of the legacy authentication procedure mutually during secure connection establishment. This important detail is the key as the attackers can masquerade as a master user to a slave device using common Bluetooth spoofing and then masquerade as slave to the legitimate master device, allowing the attacker to complete the modified session key negotiation and secure link activation between the two devices. When this exploit is successfully executed, the attacker acts as a man-in-the-middle entity to intercept critical data shared between connected devices. Additionally, the attacks can be carried out without the target being aware because the legacy standard does not require users to be notified about the outcome of an authentication procedure, or of the lack of mutual authentication.

Additionally, the BIAS attack can be chained with a Key Negotiation of Bluetooth (KNOB) attack to impersonate a Bluetooth device, complete authentication without possessing the link key, negotiate a session key with low entropy, establish a secure connection, and brute force the session key. The combination of the two attacks is novel and powerful.

Event date: May 20, 2020

Recommendations:

At this time, there have been no recorded instances of the vulnerability being exploited in the wild. To prevent attackers from utilizing the complex exploit, the researchers have notified the respective authorities to assist and coordinate issuing patches for the novel vulnerability.

In a recent press release, the Bluetooth Special Interest Group (SIG) has confirmed that they are in the process of updating the Bluetooth Core Specification to prevent BIAS attackers from downgrading the authentication method to the legacy method that attackers must utilize. Until additional guidance is provided when the SIG update is released, administrators are encouraged to:

- Keep firmware updated to the latest version and deploy new updates as soon they are approved for deployment across connected devices.
- Administrators passing critical information over Bluetooth should implement application layer authentication and encryption for the data, and only utilize Bluetooth for transport.
- At this time, the researchers have not verified the capabilities of BIAS attacks against the Bluetooth Low Energy (BLE) communication protocol commonly found in many IoT devices. The proof-of-concept cited below was performed over BD/EDR (Classic Bluetooth) by the researchers in their default configurations in their closed test environment.

Health-ISAC will share additional details and recommendations with Health-ISAC members as soon as more information regarding the Bluetooth Special Interest Group procedure update becomes available.

Sources:

References:

- Bluetooth SIG Statement Regarding the Bluetooth Impersonation Attacks (BIAS) Security Vulnerability

https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security/bias-vulnerability/

- Bluetooth devices supporting BR/EDR are vulnerable to impersonation attacks

https://www.kb.cert.org/vuls/id/647177/

- Bluetooth pairing flaw exposes devices to BIAS attacks

https://www.itpro.co.uk/security/vulnerability/355694/bluetooth-flaw-bias-attacks

- Smartphones, laptops, IoT devices vulnerable to new BIAS Bluetooth attack

https://www.zdnet.com/article/smartphones-laptops-iot-devices-vulnerable-to-new-bias-bluetooth-attack/

- New BIAS Vulnerability Affects All Modern Bluetooth Devices

https://www.cisomag.com/bias-vulnerability-affects-bluetooth-devices/

Original Research :

- Team Website and BIAS Information

https://francozappa.github.io/about-bias/

- BIAS: Bluetooth Impersonation Attacks, Daniele Antonioli, School of Computer and Communication Sciences; Nils Ole Tippenhauer, CISPA Helmholtz Center for Information Security; Kasper Rasmussen, Department of Computer Science University of Oxford

https://francozappa.github.io/about-bias/publication/antonioli-20-bias/antonioli-20-bias.pdf

- Bluetooth Impersonation Attacks (BIAS) Source Code

https://francozappa.github.io/about-bias/

- antonioli-20-bias.pdf

Please see attached.

TLP White: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions Or Comments: Please email us at toc@h-isac.org

Reference(s)

GitHubZDNetbluetoothUS-CERTIT ProCISO MagGitHub