Application Report

Bluetooth Basic Rate/Enhanced Data Rate – Bluetooth Impersonation Attacks (BIAS)

TI-PSIRT-2020-040043

CVEID: CVE-2020-10135

Publication date: May 18, 2020

Summary

Bluetooth® Special Interest Group (SIG) has issued recommendations based on findings from researchers at the École Polytechnique Fédérale de Lausanne (EPFL) regarding a potential security vulnerability, in which the attacking device spoofs the address of a previously paired remote device and successfully completes the authentication procedure with a paired/bonded device while not possessing the link key.

Affected products and versions

TI dual-mode Bluetooth controllers with BR/EDR support: CC256x, CC256xB, CC2564C, WL12xx and WL18xx.

Potentially impacted features

An attacking device would need to be within wireless range of a potentially vulnerable Bluetooth device that has bonded with a remote Bluetooth device known to the attacker. If the previous pairing procedure was completed using secure connections mode, the attacker claims to be the previously paired remote device, no longer supporting secure connections by clearing bits in its feature mask (bits 67, 136 – secure connections host and controller support). If the attacker can either downgrade authentication in this manner or attack a device that does not support secure connections, the attacker initiates a master-slave role switch to place itself into the master role and become the authentication initiator.

Suggested mitigations

Bluetooth SIG recommends that the Bluetooth Erratum 11838 be implemented to mitigate this issue. Please see the details on TI's implementation of the erratum. All TI dual-mode Bluetooth controllers have mechanisms to implement the Erratum 11838 minimum link key size, which ensures that the encryption stage exchange will fail. As a result, the attacker will be disconnected and a repairing or mutual authentication process would be needed for the device to establish a connection.

Bluetooth SIG also recommends denial of master-slave role switch during authentication and the implementation of mutual authentication. TI's dual-mode Bluetooth controllers do not allow role switch during the authentication process. However, mutual authentication has not been implemented due to tested interoperability issues. For further details on the recommendations, please see the Bluetooth SIG notice regarding the Bluetooth Impersonation Attacks (BIAS).

External references

- Bluetooth SIG notice regarding the Bluetooth Impersonation Attacks (BIAS)
- CVE-2020-10135
- École Polytechnique Fédérale de Lausanne (EPFL)

Revision history

- Version 1.0 Initial publication

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265