Application Report

Bluetooth Low Energy, Basic Rate/Enhanced Data Rate – Method Confusion Pairing Vulnerability

TI-PSIRT-2020-020038

CVEID: CVE-2020-10134

Publication date: May 18, 2020

Summary

Bluetooth® Special Interest Group (SIG) has issued recommendations based on findings from researchers at the Technical University of Munich (TUM) regarding a potential security vulnerability, enabling an attacking device to successfully intercede as a man-in-the-middle between two pairing devices. To do this, the attacker must negotiate a numeric compare procedure with one device and a passkey pairing procedure with the other, and the user must erroneously enter the numeric compare value as the passkey and accept pairing on the numeric compare device.

Potentially impacted features

An attacking device would need to be within wireless range of two vulnerable Bluetooth devices that were establishing either an LE or a BR/EDR encrypted connection using the passkey entry or numeric comparison for device authentication without existing shared credentials (LTK or link key). At least one device must permit entry of a passkey, and the other must support a display capable of representing six decimal digits.

Suggested mitigations

All devices supporting BluetoothLE Secure Connections Pairing and Secure Simple Pairing are potentially vulnerable to this attack. Bluetooth SIG suggests recommendations that can be implemented at the application layer. Please see the Bluetooth SIG notice regarding the Method Confusion pairing vulnerability for details.

External references

- Bluetooth SIG notice regarding the Method Confusion pairing vulnerability
- CVE-2020-10134
- Technical University of Munich (TUM)

Revision history

- Version 1.0 Initial publication

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), 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, 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 (www.ti.com/legal/termsofsale.html) 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.

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