Application Report

InjectaBLE: Injecting Malicious Traffic Into Established Bluetooth® Low Energy Connections

TI-PSIRT-2021-040098

CVEID: CVE-2021-31615

Publication date: June 22, 2021

Summary

Bluetooth® Special Interest Group (SIG) has issued recommendations based on findings from researchers at the LAAS-CNRS lab regarding a potential security vulnerability, which enables an attacking device to successfully inject a crafted packet into the link.

Affected products and versions

- TI *Bluetooth* Low Energy devices: CC2540, CC1352, CC1350, CC26X0, CC26X0R2 and CC26X2
- TI dual-mode *Bluetooth* controllers with *Bluetooth* Low Energy support: CC256x, CC256xB, CC2564C, WL12xx and WL18xx

CVSS base score: 6.3

CVSS vector: AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Potentially impacted features

An attacking device within wireless range of a potentially vulnerable *Bluetooth* device, following communications between a central and peripheral role, may successfully inject a crafted packet into the link. A successful packet injection to an unencrypted link may permit the attacker to spoof the central or peripheral device to the device on the opposing role. It is also possible for the crafted packets to place the attacker in a full man-in-the-middle position, allowing the attacker to modify, suppress or inject any traffic.

Suggested mitigations

There are no required fixes in the *Bluetooth* Low Energy stack or device SDK.

Bluetooth SIG suggests recommendations that can be implemented at the application layer:

- Use encryption in any profile required under specification.
- For any vendor-specific profile implementation with custom attributes, require encryption by default for both read and write operations on its characteristics.
- Give preference to use LE Secure Connections pairing using authentication and require 128-bit encryption keys, if possible.

External references

Bluetooth SIG statement regarding the "Injectable' vulnerability report

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