Application Note

Bluetooth® Classic – BrakTooth V12 Vulnerability

TI-PSIRT-2021-050100

CVEID: CVE-2021-34149

Publication date: December 30, 2021

Summary

The Bluetooth® Classic implementation on TI dual-mode Bluetooth products allows attackers in radio range to potentially trigger a denial of service of the device by flooding it with LMP_AU_Rand packets after the paging procedure. The attack causes the device to enter a deadlock state, rendering it non-responsive to the host or remote peers. Importantly, the attack is not observed to impact sensitive information within the system. As a result, the potential vulnerability has been classified as a denial of service attack and has been assigned a low priority level by TI.

CVSS base score: 6.5

CVSS vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Affected products and versions

The potential vulnerability was originally reported on TI's CC2564C device. Upon further technical analysis, TI discovered that the CC2564B, CC2564C, WL128X and WL183X devices are also impacted.

Potentially impacted features

The potential vulnerability requires the attacker to both (i) be in radio range of the Bluetooth controller and (ii) know the controller's Bluetooth device address. The devices do not have to be paired or connected. This attack disables the controller's paging, inquiry and HCI event handling.

Suggested mitigations

- Due to the low severity level of this issue, there is no plan to update or provide patches at this time.
- It is recommended that customers design their application to reboot the controller whenever there is no response to HCI commands for an extended period of time.

Acknowledgment

We would like to thank Matheus Garbelini from Singapore University of Technology and Design (SUTD) for reporting this potential vulnerability to the TI Product Security Incident Response Team (PSIRT).

External references

- BRAKTOOTH: Causing havoc on Bluetooth Link Manager

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