PSIRT Notification

Missing ECC Input Validations on CC2640 and CC2650 Devices

Summary

The SimpleLink™ CC2640 and CC2650 devices offer an Elliptic Curve Cryptography library. The following input validations are not present in that library:

Missing Validation	Validation Defined By	Impacted Functions
Private key is in range [1, n – 1]	NIST SP 800-56A Rev 3, section 5.6.2.1.2	ECCROMCC26XX_genKeys

TI PSIRT ID: TI-PSIRT-2022-040129

CVEID: None

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

CVSS base score: 6.5

Table 1-1. Affected Products

Part	Software Name	Software version	BLE Stack Name	BLE Stack Version
CC2650, CC2640	SIMPLELINK-CC2640R2-SDK: SimpleLink™ CC2640R2 SDK - Bluetooth® low energy	v5.30.00.03	BLE-Stack	v1.01.14.00
			BLE5-Stack	v3.03.08.00

Potentially Impacted Features

The following are potential impacts:

- Failure to validate private key inputs when generating the public key can result in the private key material being leaked to a malicious third party that receives the public key.
- Failure to validate private key inputs prior to generating an ECDSA signature can result in insecure signatures.

Suggested Mitigations

The following software release addresses this vulnerability. Customers can upgrade to this version to avoid this vulnerability.

Part	Software Name	Software version	BLE Stack Name	BLE Stack Version
CC2650, CC2640	SIMPLELINK-CC2640R2-SDK: SimpleLink™ CC2640R2 SDK - Bluetooth® low energy	v5.30.01.11	BLE-Stack	v1.01.15.00
			BLE5-Stack	v3.03.09.00

Customers are recommended to upgrade to the latest SDK for CC2640 and CC2650. The impacted functions are now provided with wrappers in source code to validate the inputs prior to calling the library functions.

The validation steps increase the time to perform the operations. If customers have to limit when the validation is performed, new function has been provided which do not perform the validation. Customers are encouraged to always validate the inputs at least once (for example, validate keys on first use and then store the validated keys in non-volatile memory with integrity protections for subsequent uses.)

In addition, customers are encouraged to confirm that ECC private key material is in the range [1, n -1] before using the private key in any operations.

External References

ANS X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Standard (ECDSA), November 2005.

FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013. https://doi.org/10.6028/NIST.FIPS.186-4

NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, April 2018. https://doi.org/10.6028/NIST.SP.800-56Ar3

Trademarks

SimpleLink™ is a trademark of Texas Instruments.
Bluetooth® is a registered trademark of Bluetooth SIG.
All trademarks are the property of their respective owners.

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