Application Note

Missing ECC Input Validations on CC1310 and CC1350 Devices

TI-PSIRT-2021-100118

Publication date: June 13, 2022

CVEID: None

Summary

The CC13x0 SimpleLink connected microcontrollers contain an Elliptic Curve Cryptography library in ROM. The following input validations are not present in the ROM library:

Missing Validation	Validation Defined by	Impacted Functions
Public key point is not the identity element	NIST SP 800-56A Rev 3, section 5.6.2.3.3	ECC_ECDH_computeSharedSecret, ECC_ECDSA_verify
Public key points are in the range [0, p - 1]	NIST SP 800-56A Rev 3, section 5.6.2.3.3	
Public key point is on the curve	NIST SP 800-56A Rev 3, section 5.6.2.3.3	
r and s portions of signature are in range [1, n – 1]	ANS X9.62-2005, section 7.4	ECC_ECDSA_verify
Per message secret is in range [1, n – 1]	FIPS PUB 186-4, section 6.3	ECC_ECDSA_sign
Private key is in range [1, n – 1]	NIST SP 800-56A Rev 3, section 5.6.2.1.2	ECC_generateKey

In addition, example code included in the CC1310 and CC1350 SDK incorrectly generated entropy used as an input to ECDSA sign operations, resulting in reduced protection of the private key material.

CVSS base score: 6.5

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

Affected products and versions

Part	SDK Versions	Version
CC1310, CC1350	SimpleLink™ Sub-1 GHz CC13x0 Software Development Kit	version 4.20.01.03 and earlier

While some newer parts in the CC13XX series of SimpleLink microcontrollers also contain a ROM library for ECC operations, the ROM in those newer devices do perform these input validations.

Potentially impacted features

The following are potential impacts:

- Failure to validate public key inputs during the ECDH protocol may result in private key material or shared secret material being leaked to a malicious third party.
- Failure to validate public key inputs during ECDSA verify operations may result in validating a signature that is not valid.
- Failure to validate private key inputs when generating the public key may 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 may result in insecure signatures.
- Failure to provide adequate entropy input when generating an ECDSA signature may result in the private key material being leaked.

Suggested mitigations

Customers are encouraged to upgrade to the latest SDK for CC1310 and CC1350. The impacted functions are now provided with wrappers in source code to validate the inputs prior to calling the functions in ROM.

If customers desire to limit when the validation is performed, new functions have been provided which do not perform the validation. Skipping the validation may be desirable as the validation steps increase the time to perform the operations. 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. This can be done by using the updated ECC_generateKey() function.

Finally, if customers based their application code on the “aesKeyAgreement” example included in the SDK, customers should review their code to ensure calls to ECC_ECDSA_sign() are performed correctly. Check that the 3rd parameter passed to ECC_ECDSA_sign(), the randString parameter, is formatted as follows:

- First 4 bytes of the buffer pointed to by randString contains the entropy length in 4 byte tuples,
- the remainder of the buffer contains entropy of the specified length, and
- the length of entropy is the same as the length of the private key.

For example, when using the NIST P256 curve, the randString parameter should start with: 0x08, 0x00, 0x00, 0x00 and then be followed by 32 bytes of entropy. Consult the updated example code for more details.

The following SDK releases address these vulnerabilities:

SDK	First version with mitigations
SimpleLink™ Sub-1 GHz CC13x0 Software Development Kit	4.20.02

Acknowledgment

We would like to thank Szymon Heidrich of Carrier for reporting this vulnerability to the TI Product Security Incident Response Team (PSIRT).

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

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