Application Report

Variable Time Tag Comparison on SimpleLink™ Devices

TI-PSIRT-2019-080030

Publication date: February 28, 2020

Summary

The signature verification implementation uses a non-constant time memcmp function, which enables the MAC check to be potentially vulnerable to a timing attack.

CVSS base score: 7.5

CVSS vector: https://www.first.org/cvss/calculator/3.0

Affected products and versions

- CC26X0
- CC13X0
- CC2640R2
- CC26X2
- CC13X2
- MSP432E4
- CC32XX

Potentially impacted features

- CC26X0, CC13X0: AES CCM
- CC26X2, CC13X2: AES CCM, AES GCM, ECDSA, ECJPAKE
- MSP432E4: AES CCM, AES GCM
- CC32XX: HMAC

Suggested mitigations

The following service pack releases address the potential vulnerability:

Affected SDK	SDK version with mitigation
SimpleLink CC13x2-26x2-SDK	3.30.00.03 and newer
SimpleLink MSP432E4 SDK	3.30.00.22 and newer
SimpleLink CC32xx SDK	3.30.00.04 and newer
SimpleLink CC13x0 SDK	4.10.00.10 and newer
SimpleLink CC2640R2 SDK	4.10.00.10 and newer

Acknowledgment

- TI internal finding

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