Preliminary Erratum Information Rev 0 July 2017

The erratum content below applies to the following products:

i.MX 28 i.MX 50 i.MX 53
i.MX 6QuadPlus i.MX 6DualPlus i.MX 6Quad i.MX 6Dual
i.MX 6DualLite i.MX 6Solo i.MX 6SoloLite i.MX 6SoloX
i.MX 6UltraLite i.MX 6ULL i.MX 7Dual i.MX 7Solo VFxxx (Vybrid)

ERR010873 ROM: Secure boot vulnerability when authenticating a certificate

Description

A secure boot vulnerability has been identified in the High Assurance Boot (HAB) during the parsing of a certificate in a security enabled configuration. Specific functions are used to process a certificate from its native form. Under certain conditions, it is possible to bypass the signature verification by using a specially crafted certificate. Consequently, this could lead to the execution of an unsigned and unauthorized image on the target.

Conditions

- Physical access to the target device can facilitate loading the specially crafted certificate.

- This specially crafted security certificate could also be delivered via an Over-the-Air (OTA) update. In this case, physical access to the device is not required. Designs that prevent physical access to the device and do not utilize OTA updates are not affected.

- In general, it is believed that OTA implementations will be designed such that no unauthorized material can be downloaded. However, if unrelated malware is present on the system it could by using this vulnerability potentially make itself persistent.

- Only impacts devices configured in a security enabled mode. Designs that are not using security enabled mode are not affected.

Projected Impact

The impact of this vulnerability depends on the end customer implementation.

Workarounds

- There is no software workaround available to prevent this vulnerability for the affected devices because the vulnerability is in the Boot ROM which cannot be updated in the field.

- A possible mitigation against physical (local) attacks is to prevent access to the respective SDP ports used in the final production board design.

- To prevent remote exploitation of this vulnerability for products in the field, NXP recommends that OTA mechanisms implement validity and/or conformity checks for any newly downloaded images. Such checks should already be part of the customer OTA implementation to ensure that the update was from a trusted source and not altered or corrupted. For this reason, remote access is believed to be unlikely in practical system implementations.

- For mitigation options an engineering bulletin “Mitigation for the Secure Boot Vulnerabilities (EB00854)” is available through the NXP Support channels.

Proposed Solution:

The Boot ROM on certain affected devices has been updated to prevent this vulnerability. Please contact NXP Support channels for further information on the availability of updated silicon.

Linux BSP Status:

Software workaround cannot be implemented to mask or workaround this ROM vulnerability. This erratum will result in impacted or reduced functionality as described above.

How to Reach Us:

Home Page:

nxp.com

Web Support:

nxp.com/support

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer’s technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.