Preliminary Erratum Information Rev 0 July 2017

The erratum content below applies to the following products:

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 53	**i.MX 50**	**VFxxx (Vybrid)**		

ERR010872 ROM: Secure boot vulnerability when using the Serial Downloader

Description

A secure boot vulnerability has been identified that affects the Serial Download Protocol (SDP) when the device is configured in security enabled mode. SDP could be used to download a small section of code to an unprotected region of memory. In doing so, under certain conditions, a possibility exists that this section of code could be maliciously modified to allow an unauthorized image to run.

Conditions

This security vulnerability is only present if all of the following conditions exist:

- The design is based on one of the affected SoCs listed above. Other i.MX products are not affected.
- Direct physical access to the SDP port on the target device must be available to make a serial downloader connection. Remote access to the SDP port is innately not possible. Designs without direct physical access to the SDP port are not affected.
- A specific mechanism is required to switch the target device into Serial Downloader mode, in which the SDP can run. NXP can provide details of the mechanism and guidance on methods and techniques to avoid it.
- This vulnerability only impacts devices configured in a security enabled mode. Designs 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 impacted devices, since the vulnerability is in the Boot ROM which cannot be updated in the field.

- For the i.MX 6UltraLite and i.MX 6ULL devices, a customer programmable eFUSE is available to disable the SDP port, thereby completely preventing this vulnerability.

- For other affected devices, a possible mitigation is to prevent physical access to the respective SDP ports used in the final customer production board design. NXP can provide guidance on methods to prevent physical access to the device.

- 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