Security Bulletin: CVE-2022-22819 - 11/2022

MCU ROM SB2 loader Vulnerability

A vulnerability (CVE-2022-22819) has been identified on select NXP processors by which a malformed SB2 file header sent to the device as part of an update or recovery boot can be used to create a buffer overflow. The buffer overflow can then be used to launch various exploits.

NXP recommends users review the vulnerability against their specific use cases. Each vulnerability has varying implications and reproducibility requirements, and it is up to the user to determine the impact (if any) on their products and take any necessary mitigation actions. This document will cover possible mitigations identified by NXP for the vulnerability. These mitigations may have varying applicability based on the customer's designs and should be reviewed based on the established security policy that defines the security goals of the end product.

Description and Background

The Boot ROM for select NXP devices can use SB2 (NXP Secure Boot file format, version 2.x) file format to program devices during development, manufacturing, field firmware updates, or device recovery. The normal authenticated/secure boot flow does not use the impacted SB2 file format.

The Boot ROM supports several different SB2 file loading methods:

- ISP mode: In In-System Programming (ISP) mode, the Receive SB File command (*ReceiveSbFile*) starts the transfer of an SB2 file to the target
- Recovery boot: An external SPI flash is used to store a factory image in SB2 format. When the image on the main flash is corrupted, ROM will attempt to recover the device by booting/executing the SB2 file present in the external flash device.
- ROM API: ROM on select NXP processors provides Application Programming Interfaces (APIs) intended to simplify application development and reduce the application code's footprint in flash as the API code is already in ROM. The *kb_execute/iap_api_execute* API provides in-field application update using SB2 files.

A vulnerability has been identified in the SB2 file processing. When a malformed SB2 header file is sent to the device as part of an update or recovery boot, a buffer overflow can occur. The buffer overflow can then be used to launch various exploits.

Potential Impact

The malformed SB2 header overflow can be used as part of an update or recovery boot to implement various exploits. Potential exploits include, but are not limited to enabling the debug port (if not permanently disabled using *DCFG_CC_SOCU*). If the debug port is not permanently disabled, it can potentially be re-enabled through this vulnerability and any assets accessible in system memory can potentially leak program memory (software IP) and application-specific assets. Because on-chip memory contents could leak through this exploit, an asset analysis model should be used to analyze the impact.

The vulnerability can only be exploited if SB2 files can be loaded in the final product when:

- ISP mode and/or SPI recovery boot modes are enabled
- The *kb_execute/iap_api_execute* ROM API is used

NOTE:

Normal authenticated/secure boot flow does not use the SB2 file format, so it is not directly impacted

Refer to the mitigations section for more information.

Impacted devices

Currently, all versions of the impacted devices listed below are affected. Fixes have been identified for the affected LPC and i.MX RT devices listed below. Please contact your NXP representative for scheduling and availability information of the updated devices.

NXP Device Family	Package/part number	Impacted Silicon Revisions	Fix Datecode	Mixed Datecodes
LPC55S6x, LPC55S2x	All	0A, 1B	2222	n/a
LPC55S1x, LPC55S0x	All	0A	2222	n/a
i.MX RT 500	FOWLP	B1, B2	2230	n/a
	WLCSP		2228	n/a
i.MX RT 600	MIMXRT685SFVKB	A0, B0	2222	n/a
	SC668019SFVKBR		2222	n/a

	SC668050SFFOBR		2221	2137, 2207, 2211, 2213, 2216-2220
	MIMXRT685SFFOB		2224	2211
	MIMXRT685SFAWBR		2224	n/a
	SC668016SFAWBR		2224	n/a
K32L3A	All	3N69S	n/a	n/a
K32W032S	All	3N69S	n/a	n/a
K32L3	All	All	n/a	n/a

The fixed datecodes listed above and later are guaranteed to have the latest ROM code revision with a fix for this issue. For the devices above with mixed datecode values listed for i.MX RT600, the mixed datecodes might have the fixed ROM revision, or might not. On mixed datecodes (i.MX RT600), the ROM revision must be read out using the ISP get-property command with property tag kPropertyTag_TargetVersion (0x18) to confirm if the device has the fixed ROM revision (6 or higher). Refer to the i.MX RT600 user's manual for more details on the target version property.

Mitigation

NXP has identified possible mitigations for the final production hardware to help address the vulnerability. These mitigations vary in applicability and depend on the customer's designs:

- ISP mode: Disable ISP mode by programming the boot configuration option in One-Time Programmable (OTP) or Protected Flash Region (PFR)

- Recovery boot: Disable SPI boot recovery by programming the boot configuration option in OTP or PFR

- ROM API: Call the *skboot_authenticate*() ROM API function to validate the SB2 file header before calling the *kb_execute/iap_api_execute*() ROM API function

For additional information or availability of the updated devices, please contact your NXP Account Manager or Field Representative. You can also enter a technical support ticket and an NXP support engineer will contact you.

Acknowledgment

NXP would like to thank Oxide Computer for the responsible disclosure of this vulnerability.

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.

While NXP has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer’s applications and products, and NXP accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors
www.nxp.com