Qualcomm Bootloaders

Windows Phones has had two different major bootloader revisions across its life span. Various changes have been made to the entire bootchain and emergency download 9008 technologies. For easier understanding, we will have to differentiate both bootloaders in this article.

Terminology

Starting with the Qualcomm Snapdragon 800, Qualcomm Snapdragon 610, Qualcomm Snapdragon 400 (msm8x26) and the Qualcomm Snapdragon 210 respectively, Windows Phones used a new type of bootloader we will call in this section **Bootloader Spec B**.

For the rest of the supported Qualcomm Snapdragon Processors on Windows Phone, we will call these in this section **Bootloader Spec A**.

Differences

Bootloader Spec A

Devices with a Bootloader Spec A typically include 3 Secondary bootloaders, SBL1, SBL2 and SBL3 respectively. On Bootloader Spec A devices, SBL3 can contain code for **Mass Storage mode**. The UEFI non volatile storage partitions are composed of:

- UEFI_NV
- UEFI_BS_NV
- UEFI_RT_NV
- UEFI_NV_RPMB

The format for these partitions differ with Bootloader Spec B.

These bootloaders do not implement the necessary UEFI interfaces for UEFI **Mass Storage mode** functionality to work (typically via **Mobile Startup** or **Developer Menu**) and thus can only use SBL3 mass storage implementations. They also do not implement the necessary UEFI interfaces for **Secure WIM** loading via **FFU Loader**.

Bootloader Spec B

Devices with a Bootloader Spec A typically include 1 Secondary bootloader: SBL1. No SBL3 is present, removing the ability to have a SBL3 with code for **Mass Storage mode**. The UEFI non volatile storage partitions are composed of:

- UEFI_BS_NV
- UEFI_RT_NV
- UEFI_NV_RPMB (hidden from the user portion of the eMMC)

The format for these partitions differ with Bootloader Spec B.

These bootloaders do implement the necessary UEFI interfaces for UEFI **Mass Storage mode** functionality to work (typically via **Mobile Startup** or **Developer Menu**) and can't use SBL3 mass storage implementations. They also do implement the necessary UEFI interfaces for **Secure WIM** loading via **FFU Loader**.

Exploits

Bootloader Spec A

- **UEFI non volatile storage variable duplication** (by gus33000, based on HealthCliff Spec B work)
- **SBL1 signature check bypass** (by HealthCliff)
- **Arbitrary data flashing via streaming 9008 protocol** (by HealthCliff)

Bootloader Spec B

- **UEFI non volatile storage variable duplication** (by HealthCliff)

Revision #2
Created 20 January 2020 18:13:41 by Gustave Monce
Updated 20 January 2020 18:31:42 by Gustave Monce