Modification Recommended Service Note

Supersedes:
NONE

M9537A AXIe High Performance Embedded Controller

Serial Numbers: TW00000000-TW56330709
Manufacturing ID Number: 1C00000000-1C56330709

Intel Active Management Technology Escalation of Privilege

Parts Required:

P/N	Description	Qty.

NONE

ADMINISTRATIVE INFORMATION

ACTION CATEGORY:	X ON SPECIFIED FAILURE [[]] AGREEABLE TIME	STANDARDS LABOR: 0.5 Hours			
LOCATION CATEGORY:	X CUSTOMER INSTALLABLE [[]] ON-SITE (active On-site contract required) X SERVICE CENTER [[]] CHANNEL PARTNERS	SERVICE: [[]] RETURN INVENTORY: [[]] SCRAP X SEE TEXT		USED PARTS:	[[]] RETURN [[]] SCRAP X SEE TEXT
AVAILABILITY: PRODUCT'S SUPPORT LIFE		NO CHARGE AVAILABLE UNTIL: December 1, 2018			
	[[]] Calibration Required X Calibration NOT Required	PRODUCT LINE: BL AUTHOR: TP			

ADDITIONAL INFORMATION:

KEYSIGHT TECHNOLOGIES

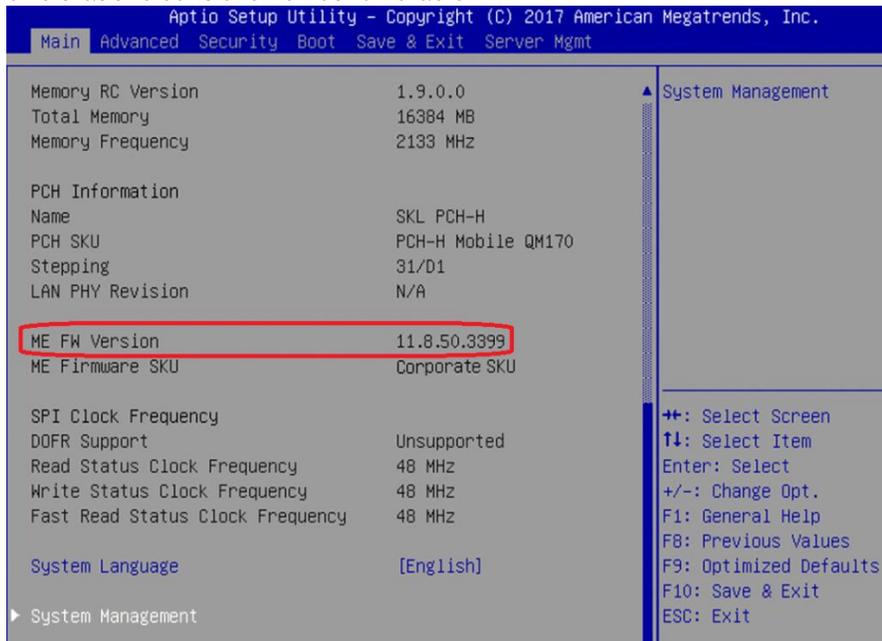## Situation:

Intel disclosed a security vulnerability in the Intel® Active Management Technology (AMT) firmware that ships in Keysight embedded controllers with affected serial numbers listed above. The vulnerability can allow an unprivileged attacker to gain control of the manageability features provided by this technology. For more information, refer to **Intel SA-00086**.

Verify that your embedded controller is not vulnerable with steps below.
1. Power on or reboot your embedded controller.
2. Press the <Delete> key when the controller beeps. This should be concurrent with the main startup screen. The BIOS setup program loads after a short delay.
3. At the BIOS Main Setup screen, verify that the "ME FW Version" is version 11.8.50.3399 or later. Below picture shows that this controller is not vulnerable.

```
              Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
    Main  Advanced  Security  Boot  Save & Exit  Server Mgmt

    Memory RC Version              1.9.0.0          ▲ System Management
    Total Memory                   16384 MB
    Memory Frequency               2133 MHz

    PCH Information
    Name                           SKL PCH-H
    PCH SKU                        PCH-H Mobile QM170
    Stepping                       31/D1
    LAN PHY Revision               N/A

    ME FW Version                  11.8.50.3399
    ME Firmware SKU                Corporate SKU

    SPI Clock Frequency
    DOFR Support                   Unsupported      →←: Select Screen
    Read Status Clock Frequency    48 MHz           ↑↓: Select Item
    Write Status Clock Frequency   48 MHz           Enter: Select
    Fast Read Status Clock Frequency  48 MHz        +/-: Change Opt.
                                                    F1: General Help
    System Language                [English]        F8: Previous Values
                                                    F9: Optimized Defaults
  ▶ System Management                               F10: Save & Exit
                                                    ESC: Exit
```

Solution/Action:

Keysight strongly recommends taking the actions specified below for embedded controllers with affected ME firmware. There are two options you can choose from to mitigate the issue.

Option 1: Update the BIOS to version SL06 or later by following the instructions at **M9537A BIOS Downloads**.
Option 2: Refer to the **Intel SA-00086** for the steps to mitigate.

Revision History:

Date	Service Note Revision	Author	Reason for Change
28 Nov 2017	01	TP	As Published