BROADCOM Release Notes: Point Release: CtrlFw_Ph_18.0_Point_Generic - 18.00.01.00 Firmware

ReleaseOrder ID:	***DCSG00930148***
Headline:	***Point Release: CtrlFw_Ph_18.0_Point_Generic - 18.00.01.00 Firmware***
Release Version:	***18.00.01.00***
UCM Project:	***CtrlFw***
Sub UCM Project:	***CtrlFw_Ph_18.0_Point_Generic***
UCM Stream:	***CtrlFw_Ph_18.0_Point_Generic***
Release Type:	***Point***
State:	***Open***
Release Baseline:	***CtrlFw_Ph_18.0_Point_Generic-2021-03-19-18.00.01.00_REL_1616138751@ \SAS35***
Release Date:	***2021-03-19 07:25:05.000000***
Date Generated:	***Mar 19, 2021***

Defects Fixed (7):

ID: DCSG00335615
Headline: SPDMLIB: Reduce number of arguments passed to IT FW debug print functions
Description Of Change: Trim down debug print message argument to 4 or less in SPDM LIB to support IT FW debug print function.
Issue Description: New debug print messages added in SPDM LIB with more than 4 arguments which exceeds number of print arguments (4) allowed in IT FW.
Steps To Reproduce: Run BMC Emulator Attestation test on IT card.

ID: DCSG00335755
Headline: MBEDTLSLIB: Compile out Mbed TLS Self-Test code
Description Of Change: Mbed TLS SelfTest code is not needed at this time, so we undefine SelfTest code to save some code space.
Issue Description: Mbed TLS SelfTest code is not needed at this time, so we undefine SelfTest code to save some code space.
Steps To Reproduce: Review the build map file and see SelfTest code is enabled.

ID: DCSG00547436
Headline: SPDM Authentication fails when BMC re-triggers SPDM Handshake
Description Of Change: In Get Version command handling in SPDM LIB, added a check if certificate buffer list is not empty when this command is received, clear out buffer list to clear any residual certificate data in the buffer. This will prevent any old certificate data from contributing to M1 computation for current Challenge command.
Issue Description: OEM BMC had out of date security root certificate in its Trust Store and controller card had updated security certificate, when this root certificate on BMC was removed and updated root certificate was added, BMC re-triggered SPDM handshake operations couple of times, but BMC failed Challenge due to signature verification failed on last Challenge command.
Steps To Reproduce: 1) Have a controller card with latest security certificate

2) Add a dummy root certificate or out of date root certificate to BMC Trust Store

3) From BMC, remove dummy or out of date root certificate, and add an updated and correct root certificate to BMC Trust Store. This will re-trigger SPDM handshake operations at least couple of time and BMC would fail the last Challenge command for signature verification fail.

ID: DCSG00908352 (Port Of Defect DCSG00555977)
Headline: [Aero][OOB] Firmware download in loop from OOB in PCIe mode fails
Description Of Change: Clear the response from the queue once the response is transmitted.
Issue Description: When FW download in loop and some Asyn requests generated by FW some time response to a FW download request is not sent because of memory shortage in response queue. Responses of few commands from the queues are not released properly.
Steps To Reproduce: 1) Download the FW via out of band in loop.
2) Observe that FW download fails after 10 cycles.

ID: DCSG00906897 (Port Of Defect DCSG00654439)
Headline: (SATA Only) IO Timeouts seen while running Unmap, SATA Passthrough and Read/Write IOs to a SATA drive
Description Of Change: When NCQ Encapsulation for SCSI Unmap command is active and a non NCQ command is received, do not send a notification for hardware to pend all new fast path IOs. This will allow SCSI Unmap command to complete and not block other non NCQ IOs.
Issue Description: If a SATA drive supports Send/Receive FPDMA Queued command, a SCSI Unmap command is translated using NCQ encapsulation with Data Set Management as subcommand of Send FPDMA Queued command. Firmware sets a flag when NCQ encapsulation is active, so that any non NCQ command received is pended while the flag is set.
However when a non NCQ command is received, a notification is sent to the hardware so any new fast path command gets pended. This results in a deadlock situation as both NCQ and non NCQ commands are not able to progress resulting in timeouts.
Steps To Reproduce: To a SATA drive that supports Send/Receive FPDMA Queued command, send a SCSI Unmap command such that it results in sending multiple Send FPDMA Queued commands. While this is in progress send some non Read/Write IOs or SATA Passthrough commands.

ID: DCSG00918083 (Port Of Defect DCSG00916381)
Headline: Controller Faults when connected to DA SEP Backplane
Description Of Change: Fixed the PL FW to make sure the DA SEP Initialize function is invoked before vSES initialize function.
Issue Description: PL FW code flow has a known restriction where in vSES initialize function should always invoked only after invoking DA SEP Initialize function. As part of PL FW code clean up, this code flow was broken and hence the controller faulted when connected to a DA SEP backplane with vSES enabled in NVData.
Steps To Reproduce: 1. Flash Phase 17 or beyond code onto the controller (Note: vSES should be enabled in NVData)
2. Connect the controller to a DA SEP Backplane

ID: DCSG00929451 (Port Of Defect DCSG00918020)
Headline: Ventura/Mercator: pl: 4311 fault
Description Of Change: Added an interlock between PCIe link down/hot reset hardware cleanup and SAS/SATA hybrid protocol mode selection to prevent the latter from attempting to change one or more phys' protocol modes while the former has placed the phy hardware in reset.
Issue Description: If both SAS/SATA and PCIe modes are enabled on device side phys and a backplane, cable, or SAS/SATA device is attached that causes PCIe receiver detection to succeed even though no PCIe device is attached, the PCIe and SAS/SATA subsystems may have an unexpected interaction that causes a 4311 fault.
Steps To Reproduce: Configure device side phys for mixed SAS/SATA/PCIe mode. Connect a backplane and SAS/SATA devices with the described property and boot the HBA.

Enhancements Implemented (4):

ID: DCSG00366048
Headline: SPDMLIB: Support SPDM Challenge command request for hash of all supported measurements
Description Of Change: Added support for computing hash of all supported measurements via Param2 field of the SPDM Challenge command.

In SPDM Lib, we would need to check for that request and compute:
hash(Concatenation(Measurement 1, Measurement 2, ..., Measurement N)) of all supported measurements.

Since Param2 field of the Challenge command can have other value, so the code has to check for other value and honors or fails the request:
0x0 = No Measurement Summary Hash,
0x1 = TCB Component Measurement Hash,
0xFF = All measurements Hash.
All other values reserved - reject SPDM Challenge command if BMC set this value in Param2.

Note:
For Aero we don't plan to support 0x1 = TCB Component Measurement Hash, so if BMC requests for this, SPDM Lib would return the hash size of all 0s. Starting in Avenger, we will support TCB.

ID: DCSG00383538
Headline: Summary of changes

Description Of Change: LIBMBEDTLS compiles for Aero using C99 but not Avenger which uses CPP.
The changes consist mostly of:

1.) Casts to set the variable type correctly for various assignments and function calls.
2.) Dealing with unused variables/parameters in a benign way.

ID: DCSG00813882

Headline: MBEDTLS LIB: Add license files to source tree

Description Of Change: Add license files to MBEDTLS LIB source tree: apache-2.0.txt and LICENSE.

ID: DCSG00645950 (Port Of EnhancementRequest DCSG00500296)

Headline: [SPDM] Blocking slots 1-7 from configuring SPDM certificates

Description Of Change: As per OEM request blocking the certificate slots 1 to 7. Only slot 0 should be in use.
If the users attempt to send a command to program certificate from slot 1 - 7, FW will reject this command with invalid parameter status.
