

	<p>10. Modified SPS version strings and removed the "Manufacturer ID" string.</p> <p>11. Disabled support for EFI iSCSI.</p> <p>12. Updated SmcOOB module to 1.01.24 to support SUM clean SMBIOS Event log through BiosCfg header flag.</p> <p>13. Added support for EUI-48 Locally Administered MAC Address for Redfish host interface.</p> <p>14. Enhanced DMI type 42 for supporting EUI-48 Locally Administered MAC Address.</p>
New features	N/A
Fixes	<p>1. Fixed inability of NumLock item to modify by SmcPostHotKey.sd.</p> <p>2. Fixed failure of SUM TC 221 when installing multiple NICs on system.</p> <p>3. Fixed inability to preserve SGX settings after updating BIOS.</p> <p>4. Fixed problem of the system hanging during POST when building BIOS with the token "SMC_SETUP_STYLE" as 0.</p> <p>5. Fixed malfunction of Patrol Scrub on Dx ICX.</p> <p>6. Corrected firmware version and vendor on Trusted Computing page.</p> <p>7. Fixed inability to change COM port resource and failure of item's behavior.</p> <p>8. Fixed problem of the system continuously rebooting when AOC-A25G-i2SM or AOC-A25G-M2SM is plugged in.</p> <p>9. Set bits of IPMI CMD 30_A0_15 to clear according to usage of location instead of all bytes.</p> <p>10. Updated eSPI maximum I/O mode for slave 0 (BMC).</p>

Release Notes from Previous Release(s)

1.1 (5/6/2021)

1. Set default Boot Guard profile to 5.
2. Updated Intel-Generic-Microcode.
3. Updated ASPEED VBIOS and EFI driver to 1.11.03.
4. Updated SATA/ssATA EFI driver to VROC PreOS v7.5.0.1152.
5. Kept value of setup string of Manufacturer and Product according to priority "modification of AmiBcp, FRU1, and then SMBIOS Table".
6. Added code to stop AFU support.
7. Added HCC Mx stepping CPU check for CPU stepping display.
8. Automatically disabled and hid ADDDC with x8 width DIMM.
9. Set "NVMe Firmware Source" to auto-hide when AOC-SMG3-2M2-B is plugged in.
10. Disabled MCTP for M.2 slots to prevent system hang with Micron 2300.
11. Removed 4G limit of Intel LAN memory if boot mode is not legacy.
12. Automatically disabled and grayed out ADDDC, UMA-Base Clustering, and mirror mode and enabled NUMA when SGX is enabled.
13. Enhanced SMCI HDD Security feature.
14. Extended memory DIMM serial number information (Samsung, Micron, Hynix).
15. Enhanced SMC DCPMM feature.
16. Set all OPRM control items to Legacy when boot mode is set to Dual.
17. Updated CPLD Signature table 101 and tool to 1.30.24 for CPLD Signature.
18. Updated Intel BKCWW17 2021 PV MR1.
19. Hid eADR Support item.
20. Updated SPS 4.4.4.56 PV MR2.
21. Corrected display of IPv4 address source status after updating BIOS.
22. Fixed missing SMBIOS type 17 BPS information when plugged in at P1-DIMMC2 or P2-DIMMC2.
23. Corrected location of RT UECC log.
24. Fixed failure of RT UECC to be mapped out.
25. Corrected display of IPv6 when IPv6 status is not active.
26. Filtered Dynamic HDD Security pages to patch failure of SUM ChangeBiosCfg.
27. Fixed problem of T-states always showing 15 levels even when T-state is disabled.
28. Fixed problem with a CPU exception.
29. Fixed failure to hide the SmcSecureErase setup page when no HDD devices are plugged in.
30. Corrected display of UEFI OS boot option name in BIOS setup.
31. Fixed failure of Secure Boot Append/Update Keys.
32. Fixed inability to upload all OOB files on the first BMC boot.
33. Corrected memory device number in SMBIOS type 16.
34. Corrected iSCSI Configuration page.
35. Set DIMM size to recalibrate when rank is disabled.
36. Fixed the issue of system hanging after executing sum -c EraseOAKey or afuefi /OAD.
37. Added workaround for issue of updating BIOS then rebooting causing system CPU exception at 0x79 when TXT is enabled.

1.0a (1/13/2021)

1. Updated WW51.
2. Added support for BIOS uploading/downloading OOB file to/from BMC during POST even if SMCI USB Redfish Host Interface is set to "OFF" in IPMI GUI web.
3. Fixed problem of system hanging at 0xB2 when plugging in the SATA and NVMe device.
4. Added force next boot to UEFI Shell support.

5. Implemented CPU always turbo function.
6. Added support for Linux built-in utility efibootmgr.
7. Filled Onboard LAN1 MAC address into SMBIOS Type 1 UUID field.
8. Set CMOS Battery Low event to log into SMBIOS (POST Error Type 08h).
9. Added support for changing PXE from UEFI (U)/Legacy (L) to L/U through IPMI Boot Flag Command.
10. Enabled OOB file to be uploaded/downloaded to/from BMC even if Network Stack is disabled.
11. Fixed inability of the system to boot into PXE with DVD installed.
12. Enhanced SMCI HDD Security feature.
13. Set PCLS and ADDDC to enabled by default and enabled leaky bucket of about 2.15 minutes.
14. Added Enhance PPR function.
15. Added Auto mode to "NVMe Mode Switch".
16. Added SEL for PPR success.
17. Fixed inability to find "Rear USB Port(s)" for SUM test case 343.
18. Fixed problem of system hanging at postcode "B2" when creating RAID0/1 volume.
19. Fixed problem of system exception occurring at 0x92 or 0xA2 after changing boot order and rebooting.
20. Fixed inability to correctly set some DMI data.
21. Fixed problem of system exception occurring and rebooting when using IPMI force boot to UEFI disk.
22. Fixed problem of system hanging if moving USB KB/MS when entering Windows.
23. Fixed malfunction of setup item "Maximum Read Request".
24. Corrected display of IPv6 in Early Video.
25. Fixed problem of "Configuration Address Source" always showing "DHCP" on IPMI IPv6 page.
26. Corrected Memory Correct Error location in BIOS event log for CPU2.
27. Modified IPv6 behavior to remove error message when IPv6 router IP is ::::.
28. Corrected CPU1 memory type 20 handler point to CPU2 Memory Array Mapped Address structure.
29. Corrected display of IPv6 Status after updating BIOS.

1.0 (8/26/2020)

Initial release.