IPMI Firmware / BIOS Release Notes Form

Supermicro disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.

Product Name	**H11DST-B (2.0)**
Release Version	**3.0**
Release Date	**07/26/2024**
Previous Version	**2.8**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**ECO #30523** **BIOS_H11DSTB-098A_20240726_3.0_STDsp.bin** **Please update BIOS with attached Flash Utility in package.** **Note: BIOS R 2.x /3.x only supports MB Rev. 2.00, with 32MB SPI flash ROM to support both AMD 7001/7002 series processors.**
Enhancements	1. Update SA50232_Supplement(Vulnerabilities in EDK2 NetworkPkg). 2. Update AGESA NaplesPI to 1.0.0.M based on 5.013_NaplesCrb_0ACIJ032 and Security Update for SA50158. 3. Enable ASPM in ACPI FACP when pcie ASPM is enabled. 4. Add SMC Debug log support. 5. Update AMI Modules based on 5.14_RomeCrb_0ACMK030 and Small Adjustments for Security Update SA50216 and SA50218. 6. Set Chassis type in smbios to default (0x11) when Chassis type from fru is 0x00 or 0xFF or NULL. 7. Fix "Check Secure Encrypted Virtualization Function" fail(Projects that are not ROT will encounter problems). 8. Fill DUID with UUID to avoid all system's DUID in IPv6 DHCP is the same ; The DUID in IPv6 DHCP should be unique. 9. Update AMI Modules based on 5.14_RomeCrb_0ACMK031, Security Update for SA50258 10. Update AMI Modules based on 5.14_RomeCrb_0ACMK032, Update AGESA RomePI to 1.0.0.J and Security Update for SA50158. 11. Update SA50121_Supplement(TOCTOU Vulnerability). 12. Update SA50230_Supplement(Image Parser Corruption Vulnerability). 13. Update SA50235_Supplement(Extended Image Parser Corruption Vulnerability) to address 14. Update secure boot KEK and DB (Fellow EagleStream SVN 2926). 15. Added SmcBootModeCallBack function for setup item "boot mode" to auto switch the option roms' value. 16. Update SA50221_Supplement(UsbRt SMM Vulnerability Arbitrary Code Execution). 17. Update SA50215_Supplement(Buffer Overflow Vulnerability in SmmLockBox). 18. Update SA50243_Supplement(UsbRt TOCTOU Vulnerability). 19. Update AMI Modules based on 5.14_RomeCrb_0ACMK029. 20. Update AMI Modules based on 5.14_RomeCrb_0ACMK030.
New features	**N/A**

Fixes	1. Avoid to recover priority of inter-group when persistent is set. (Sync Whitley SVN 2223) 2. When IPMI send persistent flag, user cannot change boot option at next boot ; Adjust rule of IpmiBootFlag about clearing valid bit after CMD is executed and not locking priority of inter-groups after CMD is executed with persistent flag 3. Fixes the system would reboot during flash BIOS with watchdog function enable. 4. Fixed memory multi-bit error will report to correctable error.

Release Notes from Previous Release(s)

2.8 (12/14/2023)
1. Update SA50232_Supplement(Vulnerabilities in EDK2 NetworkPkg); Quarkslab identified two weaknesses related to predictable TCP initial sequence numbers due to using a cryptographically weak pseudo-random number generator.
2. Update AGESA NaplesPI to 1.0.0.M based on 5.013_NaplesCrb_0ACIJ032 and Security Update for SA50158.
3. Enable ASPM in ACPI FACP when pcie ASPM is enabled.
4. Add SMC Debug log support ; Control by hidden setup item "CPU Debug Log Support" default Disabled.
5. Update AMI Modules based on 5.14_RomeCrb_0ACMK030 ; Small Adjustments for Security Update SA50216 and SA50218.
6. Set Chassis type in smbios to default (0x11) when Chassis type from fru is 0x00 or 0xFF or NULL.
7. Fix "Check Secure Encrypted Virtualization Function" fail(Projects that are not ROT will encounter problems) ; SEV data need to be preserve when afu tool flash BIOS.
8. Fill DUID with UUID to avoid all system's DUID in IPv6 DHCP is the same ; The DUID in IPv6 DHCP should be unique.
9. Update AMI Modules based on 5.14_RomeCrb_0ACMK031 ; Security Update for SA50258.
10. Update AMI Modules based on 5.14_RomeCrb_0ACMK032 ; Update AGESA RomePI to 1.0.0.J and Security Update for SA50158.
1. Avoid to recover priority of inter-group when persistent is set. (Sync Whitley SVN 2223) ; When force persistent command by IPMI, don't save current Boot Order for use on the next boot.
2. When IPMI send persistent flag, user cannot change boot option at next boot ; Adjust rule of IpmiBootFlag about clearing valid bit after CMD is executed and not locking priority of inter-groups after CMD is executed with persistent flag

2.7 (10/23/2023)
1. Updated AGESA RomePI to 1.0.0.F based on 5.14_RomeCrb_0ACMK026 for AMD-SB-1032.
2. Added Rocky Linux boot option name.
3. Updated Rome B0 stepping CPU microcode 0x0830107A from AMD-SB-7008 Security Bulletin to address CVE-2023-20593 issue.
4. Restored SMCI secure boot keys and updated Secure Boot DB variable. (Unknown certificate "Addtrust External CA Root" expired on May 30, 2020).
5. Updated AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
6. Changed Pxe from Uefi(U)/Legacy(L) to L/U through Redfish.
7. Added InBand OemFID support.
8. Added OutBand OemFID support.
9. Updated OEM FID information for PRICESSO_0_DESC and PRICESSO_1_DESC.
10. Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C.

2.5 (10/27/2022)
1. Changed BIOS revision to 2.5.
2. Updated AGESA NaplesPI to 1.0.0.H.
3. Updated 8012 ZP-B2 microcode 0800126E.
4. Updated 8310 SSP-B0 microcode 8301052.
5. Set Relaxed Ordering default to Enabled.
6. Added Setup item "Enhanced Preferred IO Mode".
7. Updated DBX file to fix Secure Boot Bypass issue.
8. Updated AGESA RomePI to 1.0.0.E based on 5.14_RomeCrb_0ACMK025.
9. Updated Rome B0 stepping CPU microcode 0x08301055 to patch Errata 1161, 1176, 1179, 1183, 1214, 1268, 1386, 1417.
10. Modified Setup string naming from SMCI to Supermicro.
11. Removed "Vendor Keys" in security page.

2.3 (11/25/2022)
1. Changed BIOS revision to 2.3.
2. Updated AGESA RomePI to 1.0.0.9.
3. Updated 8310 SSP-B0 microcode 830104D.
4. Exposed the items below for GPU performance tuning • TSME • DDR Power Down Enable • PCIe Ten Bit Support

2.2 (8/28/2020)
1. Changed BIOS revision to 2.2.
2. Updated AGESA RomePI to 1.0.0.8.
3. Updated 8310 SSP-B0 microcode 8301038.
4. Updated AGESA NaplesPI to 1.0.0.D.
5. Updated 8012 ZP-B2 microcode 0800126C.
6. Fixed problem of system hanging on POSTCODE 0xB2 when JPG1 is set to disabled and the VGA card is plugged in.

7. Added SMCI HDD Security feature.
8. Updated help string of item "Input the description".
9. Fixed failures of FRU0 - Manufacturer Name (PM) to sync to SMBIOS Type 3 - Manufacturer (CM) and FRU0 - Product Part/Model Number (PPM) to sync to SMBIOS Type 1 - ProductName (PN).
10. Removed "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
11.Added AMD IOMMU patch code to
12.fix NVMe Devices drop and Hardware error in RH 7.x. 12. Fixed problem of TCG admin password reverting.
13. Corrected CPU speed information in BIOS setup

2.1 (2/21/2020)
1. Changed BIOS revision to 2.1. 2. Updated AGESA RomePI to 1.0.0.5 based on 5.14_RomeCrb_0ACMK013. 3. Displayed "PCI AER Support" setup item on ACPI page. 4. Added SMC HDD Security feature. 5. Fixed issue of system hanging at post code A7h. 6. Fixed inability of SUM to change the function of NUMA Node Per Socket. 7. Fixed problem of system sometimes rebooting during legacy Windows 2019 OS installation when using Rome CPU 7502. 8. Removed requirement to use Admin password for erasing TCG device.

2.0b (11/15/2019)
1. Changed BIOS revision to 2.0b.
2. Added "DRAM Scrub Time" to Memory Configuration.
3. Updated AGESA RomePI to 1.0.0.4 based on 5.14_RomeCrb_0ACMK012.
4. Set AMD CBS "PCIe ARI Support" item to be used instead of "ARI Forwarding".
5. Updated item string "Input the description" and "HTTP Boot One Time" to adhere to Rome BIOS Setup Template v0.7_20190705.
6. Displayed 3rd IPMI version in BIOS setup.
7. Updated SSID of AMD Host Bridge according to each project's board ID.
8. Set IOMMU default to Auto (Enabled)
9. Displayed "Preferred IO" item.
10. Prevented display of any AMD memory error messages during the POST phase.
11. Fixed malfunction of recovery.
12. Added support for OOB SATA HDD information and asset information of 2 SATA controllers.
13. Fixed missing screen output when Boot Mode is changed to EFI.
14. Fixed the issue of "SMCI POST Screen Message" appearing on BIOS setup menu.
15. Fixed the issue of "SMCI POST Screen Message" appearing on POST screen when executing EFI Shell application.

2.0 (9/12/2019) Initial Release