# 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** | **H11DSi/H11DSi-NT** |
| **Release Version** | **3.0** |
| **Release Date** | **07/12/2024** |
| **Build Date** | **07/12/2024** |
| **Previous Version** | **2.8** |
| **Update Category** | **Recommended** |
| **Dependencies** | **MB Rev 2.00** |
| **Important Notes** | **BIOS Image:**<br>**BIOS_H11DSI-0964_20240712_3.0_STDsp.bin**<br>**BIOS Update Package:**<br>**BIOS_H11DSI-0964_20240712_3.0_STDsp.zip**<br>**Note:**<br>**BIOS R 2.x only supports MB Rev. 2.00, with 32MB SPI flash ROM to support both AMD 7001/7002 series processors.** |
| **Enhancements** | **1. [Naples][Enhancements] Update SA50232_Supplement(Vulnerabilities in EDK2 NetworkPkg).**<br>**2. [Naples][Enhancements] Update AGESA NaplesPI to 1.0.0.M based on 5.013_NaplesCrb_0ACIJ032.**<br>**3. [Rome][Enhancements] Enable ASPM in ACPI FACP when pcie ASPM is enabled.**<br>**4. [Rome][Enhancements] Add SMC Debug log support.**<br>**5. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK030.**<br>**6. [Rome][Enhancements] Set Chassis type in smbios to default (0x11) when Chassis type from fru is 0x00 or 0xFF or NULL.**<br>**7. [Rome][Enhancements] Fix "Check Secure Encrypted Virtualization Function" fail(Projects that are not ROT will encounter problems).**<br>**8. [Rome][Enhancements] Fill DUID with UUID to avoid all system's DUID in IPv6 DHCP is the same.**<br>**9. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK031.**<br>**10. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK032.**<br>**11. [Naples][Rome][Enhancements] Update SA50218_Supplement(Vulnerabilities in EDK2 NetworkPkg).**<br>**12. [Naples][Enhancements] Update SA50121_Supplement(TOCTOU Vulnerability).** |

| | |
|---|---|
| | 13. [Naples][Rome][Enhancements] Update SA50230_Supplement(Image Parser Corruption Vulnerability).<br>14. [Naples][Rome][Enhancements] Disable ASPM in ACPI FACP when pcie ASPM is disabled.<br>15. [Naples][Rome][Enhancements] Update SA50235_Supplement(Extended Image Parser Corruption Vulnerability) to address<br>16. [Naples][Rome][Enhancements] Update secure boot KEK and DB (Fellow EagleStream SVN 2926).<br>17. [Naples][Enhancements] Added SmcBootModeCallBack function for setup item "boot mode" to auto switch the option roms' value.<br>18. [Naples][Enhancements] Update SA50221_Supplement(UsbRt SMM Vulnerability Arbitrary Code Execution).<br>19. [Naples][Enhancements] Update SA50215_Supplement(Buffer Overflow Vulnerability in SmmLockBox).<br>20. [Naples][Enhancements] Update SA50243_Supplement(UsbRt TOCTOU Vulnerability).<br>21. [Rome][Enhancements] Enhance get VPD data routines for E710.<br>22. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK029.<br>23. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK030. |
| New features | NA |
| Fixes | 1. [Naples][Fixes] Avoid to recover priority of inter-group when persistent is set. (Sync Whitley SVN 2223)<br>2. [Naples][Rome][Fixes] When IPMI send persistent flag, user cannot change boot option at next boot.<br>3. [Naples][Fixes] System would reboot during flash BIOS with watchdog function enable.<br>4. [Rome][Fixes] Fixed memory multi-bit error will report to correctable error. |

*2.8 (12/14/2023)*

1. Updated AGESA RomePI to 1.0.0.H based on 5.14_RomeCrb_0ACMK028.
2. Updated AGESA NaplesPI to 1.0.0.L based on 5.013_NaplesCrb_0ACIJ031.
3. Updated SA50216_Supplement(LogoFAIL Vulnerability).
   Disabled "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support"
4. Fixed MP1(SMU) and CPU WDT uncorrectable error,  “no event log” issue.

*2.7 (10/25/2023)*

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 30th 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. Updated the DBX file to fix Secure Boot Bypass issue.
2. Updated AGESA RomePI to 1.0.0.E based on 5.14_RomeCrb_0ACMK025.
3. Updated Rome B0 stepping CPU microcode 0x08301055 to patch Errata 1161, 1176, 1179, 1183, 1214, 1268, 1386, 1417.
4. Changed setup string title from “SMCI” to “Supermicro”.
5. Removed "Vendor Keys" in security page.

*2.4 (12/28/2021)*

1. Changed BIOS revision to 2.4
2. Updated AGESA NaplesPI to 1.0.0.H.
3. Updated the 8012 ZP-B2 microcode to 0800126E.
4. Updated the AGESA RomePI to 1.0.0.D.
5. Updated the 8310 SSP-B0 microcode to 8301052.
6. Set Relaxed Ordering default to “Enabled”.
7. Added setup item: "Enhanced Preferred IO Mode".

*2.3 (8/2/2021)*

1. Updated AGESA NaplesPI to 1.0.0.D.
2. Updated 8012 ZP-B2 microcode 0800126C.
3. Fixed problem of system hanging on POSTCODE 0xB2 when JPG1 is set to disabled and the VGA card is plugged in.
4. Added SMCI HDD Security feature.
5. Updated help string of item "Input the description".
6. Changed BIOS revision to 2.3.
7. Updated AGESA RomePI to 1.0.0.9.
8. Updated 8310 SSP-B0 microcode 830104D.
9. Updated Byte6 setting and Byte12 setting of slave address C0h and C2h SATA redriver from 0xE1 to 0xC1.

10. 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).
11. Removed "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
12. Added AMD IOMMU patch code to fix NVMe Devices drop and Hardware error in RH 7.x.
13. Fixed problem of TCG admin password reverting.
14. Corrected CPU speed information in BIOS setup.
15. Fixed inability to detect SATA device (CPU1 SATA0-3) during Ubuntu 20.10 installation when networking AOC (AOC-STGS-i2T) is plugged into Slot 5.
16. Rolled back SmcHttpBoot module to fix problem of BIOS flash from 2.1 to 2.3 hanging up and erasing all blocks in Non-Boot with Rome CPU.

*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 (11/19/2019)*

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. Forced all PCIe to Gen3 only for H11 drop-in projects.
9. Displayed the "4-link xGMI max speed" setup item and set to 10.667Gbps by default on H11 DP drop-in projects.
10. Set IOMMU default to Auto (Enabled)
11. Displayed "Preferred IO" item.
12. Prevented display of any AMD memory error messages during the POST phase.
13. Fixed malfunction of recovery.
14. Added support for OOB SATA HDD information and asset information of 2 SATA controllers.
15. Fixed missing screen output when Boot Mode is changed to EFI.
16. Fixed problem of system hanging when installing NVidia RTX 2080/5000/6000.
17. Fixed the issue of "SMCI POST Screen Message" appearing on BIOS setup menu.
18. Fixed the issue of "SMCI POST Screen Message" appearing on POST screen when executing EFI Shell application.
19. Corrected the CPM table setting.
20. Fixed failure of iSCSI function when LAN option is in UEFI mode.
21. Fixed problem of the xGMI speed reaching 16G after pressing “load default.”
22. Fixed problem of the default xGMI speed not being 10.6G.
23. Fixed problem of yellow exclamation mark appearing in Windows 2019 Device Manager when running AST2500 VGA UEFI OPROM on NBIO1.
24. Fixed inability to detect NVMe device on P2_NVME0 and P2_NVME1 ports.

*2.0 (9/25/2019)*

Initial Release