BIOS Release Notes Form

Product Name	**H11DSU-iN**
Release Version	**3.3**
Release Date	**03/28/2025**
Previous Version	**3.2**
Update Category	**Recommended**
Dependencies	**MB Rev 2.10**
Important Notes	**BIOS R3.0 and newer only support MB Rev2.10 with 32MB SPI flash ROM to support both AMD 7001/7002 series processors** **BIOS image: BIOS_H11DSU-0963_20250328_3.3_STDsp.bin** **BIOS image and flash utility package: BIOS_H11DSU-0963_20250328_3.3_STDsp.zip**
Enhancements	1. [Naples][Enhancements] Update SA50299 to address CVE-2025-22830(High, 7.3) 2. [Naples][Enhancements] Update AGESA NaplesPI to 1.0.0.Q based on (BETA)5.013_NaplesCrb_0ACIJ035. 3. [Rome][Enhancements] Update AMI Modules based on (BETA)5.14_RomeCrb_0ACMK035. 4. [Rome][Enhancements] Update Legacy Serial Redirection module from MAINT_LegacySreDir_13.01 to MAINT_LegacySreDir_14.01 5. [Naples][Rome][Enhancements] Update Secure Boot DBX to address AMI SA50300 (CVE-2024-7344\CVE-2023-24932 (8.2 High/6.7 Middle) security issue
New features	N/A
Fixes	N/A

3.2 (07/12/2024)

1. [Naples][Rome][Enhancements] Update SA50289(TianoCompress Privilege Escalation Vulnerability) to address CVE-119
2. [Naples][Enhancements] Update AGESA NaplesPI to 1.0.0.P based on 5.013_NaplesCrb_0ACIJ034.

3. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK034.

3.1 (10/21/2024)

1. [Naples][Enhancements] Update AGESA NaplesPI to 1.0.0.N based on 5.013_NaplesCrb_0ACIJ033.
2. [Naples][Enhancements] Merge SA50191 code change
3. [Naples][Enhancements] Update SA50273 (OpenSSL Vulnerabilities) to address CVE-2006-7250(Medium, 5.0), CVE-2009-1377(Medium, 5.0), CVE-2009-1378(Medium, 5.0), CVE-2009-1387(Medium, 5.0), CVE-2009-3245(High, 10.0), CVE-2009-4355(Medium, 5.0), CVE-2010-0433(Medium, 4.3), CVE-2010-0740(Medium, 5.0), CVE-2010-0742(High, 7.5), CVE-2010-3864(High, 7.6), CVE-2010-4180(Medium, 4.3), CVE-2011-0014(Medium, 5.0), CVE-2011-3210(Medium, 5.0), CVE-2011-4108(Medium, 4.3), CVE-2011-4109(High, 9.3), CVE-2012-0884(Medium, 5.0), CVE-2012-1165(Medium, 5.0), CVE-2012-2110(High, 7.5), CVE-2012-2333(Medium, 5.0), CVE-2013-0166(Medium, 5.0), CVE-2013-0169(Low, 2.6), CVE-2014-0195(Medium, 6.8), CVE-2014-0221(Medium, 4.3), CVE-2014-0224(High, 7.4), CVE-2014-3470(Medium, 4.3), CVE-2014-8176(High, 7.5), CVE-2015-0292(High, 7.5), CVE-2014-3505(Medium, 5.0), CVE-2014-3506(Medium, 5.0), CVE-2014-3507(Medium, 5.0), CVE-2014-3508(Medium, 4.3), CVE-2014-3510(Medium, 4.3), CVE-2014-3568(Medium, 4.3), CVE-2014-3567(High, 7.1), CVE-2014-3570(Medium, 5.0), CVE-2014-3571(Medium, 5.0), CVE-2014-3572(Medium, 5.0), CVE-2014-8275(Medium, 5.0), CVE-2015-0204(Medium, 4.3), CVE-2015-0209(Medium, 6.8), CVE-2015-0286(Medium, 5.0), CVE-2015-0287(Medium, 5.0), CVE-2015-0288(Medium, 5.0), CVE-2015-0289(Medium, 5.0), CVE-2015-0293(Medium, 5.0), CVE-2016-0703(Medium, 5.9), CVE-2016-0704(Medium, 5.9), CVE-2011-1945(Low, 2.6), CVE-2015-1789(High, 7.5), CVE-2015-1790(Medium, 5.0), CVE-2015-1791(Medium, 6.8), CVE-2015-1792(Medium, 5.0), CVE-2015-1794(Medium, 5.0), CVE-2015-3193(High, 7.5), CVE-2015-3194(High, 7.5), CVE-2015-3195(Medium, 5.3), CVE-2015-3197(Medium, 5.9), CVE-2016-0701(Low, 3.7), CVE-2016-0702(Medium, 5.1), CVE-2016-0705(High, 9.8), CVE-2016-0797(High, 7.5), CVE-2016-0798(High, 7.5), CVE-2016-0799(High, 9.8), CVE-2016-0800(Medium, 5.9), CVE-2016-2842(High, 9.8), CVE-2016-2105(High, 7.5), CVE-2016-2106(High, 7.5), CVE-2016-2107(Medium, 5.9), CVE-2016-2109(High, 7.5), CVE-2016-2176(High, 8.2), CVE-2016-2182(High, 9.8), CVE-2016-6302(High, 7.5), CVE-2016-2177(High, 9.8), CVE-2016-2178(Medium, 5.5), CVE-2016-2179(High, 7.5), CVE-2016-2180(High, 7.5), CVE-2016-2181(High, 7.5), CVE-2016-2183(High, 7.5), CVE-2016-6306(Medium, 5.9), CVE-2020-1968(Low, 3.7), CVE-2017-3737(Medium, 5.9), CVE-2017-3731(High, 7.5), CVE-2017-3735(Medium, 5.3), CVE-2018-0739(Medium, 6.5), CVE-2018-0732(High, 7.5), CVE-2018-5407(Medium, 4.7), CVE-2018-0734(Medium, 5.9), CVE-2019-1543(High, 7.4), CVE-2019-1547(Medium, 4.7), CVE-2019-1563(Low, 3.7), CVE-2020-1967(High, 7.5), CVE-2020-1971(Medium, 5.9), CVE-2021-23840(High, 7.5), CVE-2021-23841(Medium, 5.9), CVE-2021-3449(Medium, 5.9), CVE-2021-3450(High, 7.4), CVE-2021-3711(High, 9.8), CVE-2021-3712(High, 7.4), CVE-2022-0778(High, 7.5), CVE-2022-4450(High, 7.5), CVE-2023-0215(High, 7.5), CVE-2023-0286(High, 7.4), CVE-2023-0464(High, 7.5), CVE-2023-0465(Medium, 5.3) security issue.

4. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK033.

3.0 (07/12/2024)

1. [Naples][Enhancements] Update SA50232_Supplement(Vulnerabilities in EDK2 NetworkPkg).
2. [Naples][Enhancements] Update AGESA NaplesPI to 1.0.0.M based on 5.013_NaplesCrb_0ACIJ032.
3. [Rome][Enhancements] Enable ASPM in ACPI FACP when pcie ASPM is enabled.
4. [Rome][Enhancements] Add SMC Debug log support.
5. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK030.
6. [Rome][Enhancements] Set Chassis type in smbios to default (0x11) when Chassis type from fru is 0x00 or 0xFF or NULL.
7. [Rome][Enhancements] Fix "Check Secure Encrypted Virtualization Function" fail(Projects that are not ROT will encounter problems).
8. [Rome][Enhancements] Fill DUID with UUID to avoid all system's DUID in IPv6 DHCP is the same.
9. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK031.
10. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK032.
11. [Naples][Rome][Enhancements] Update SA50218_Supplement(Vulnerabilities in EDK2 NetworkPkg).
12. [Naples][Enhancements] Update SA50121_Supplement(TOCTOU Vulnerability).
13. [Naples][Rome][Enhancements] Update SA50230_Supplement(Image Parser Corruption Vulnerability).
14. [Naples][Rome][Enhancements] Disable ASPM in ACPI FACP when pcie ASPM is disabled.
15. [Naples][Rome][Enhancements] Update SA50235_Supplement(Extended Image Parser Corruption Vulnerability) to address
16. [Naples][Rome][Enhancements] Update secure boot KEK and DB (Fellow EagleStream SVN 2926).
17. [Naples][Enhancements] Added SmcBootModeCallBack function for setup item "boot mode" to auto switch the option roms' value.
18. [Naples][Enhancements] Update SA50221_Supplement(UsbRt SMM Vulnerability Arbitrary Code Execution).
19. [Naples][Enhancements] Update SA50215_Supplement(Buffer Overflow Vulnerability in SmmLockBox).
20. [Naples][Enhancements] Update SA50243_Supplement(UsbRt TOCTOU Vulnerability).
21. [Rome][Enhancements] Enhance get VPD data routines for E710.
22. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK029.
23. [Rome][Enhancements] Update AMI Modules based on 5.14_RomeCrb_0ACMK030.
24. [Naples][Fixes] Avoid to recover priority of inter-group when persistent is set. (Sync Whitley SVN 2223)
25. [Naples][Rome][Fixes] When IPMI send persistent flag, user cannot change boot option at next boot.
26. [Naples][Fixes] System would reboot during flash BIOS with watchdog function enable.

27. [Rome][Fixes] Fixed memory multi-bit error will report to correctable error.

2.8 (12/14/2023)

1. [Rome][Enhancements] Update AGESA RomePI to 1.0.0.H based on 5.14_RomeCrb_0ACMK028.
2. [Rome][Fixes] Fixed the problem that the AMD Radon PRO W7500 & W7600 VGA card cannot be displayed in the shell or BIOS setup menu.
3. [Naples][Enhancements] Update AGESA NaplesPI to 1.0.0.L based on 5.013_NaplesCrb_0ACIJ031.
4. [Naples][Rome][Enhancements] Update SA50216_Supplement(LogoFAIL Vulnerability).
5. [Rome][Enhancements] Fixed MP1(SMU) and CPU WDT uncorrectable error no event log issue.
6. [Rome][Enhancements] Disable "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" set Disabled.

2.7 (10/20/2023)

1. [Rome][Enhancements] Update AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
2. [Rome][SmcOptIpmiBoot][Enhancements] Support that changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish.
3. [Naples][Rome][Fixes] Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C.
4. [Naples][Enhancements] Enable token ASM1061_Workaround to disable ASM1061 64-bit memory address capability.

2.6a (09/27/2023)

1. [Enhancements][Rome BIOS] Update AGESA RomePI to 1.0.0.F based on 5.14_RomeCrb_0ACMK026 for AMD-SB-1032.
2. [Enhancements][Naples/Rome BIOS] Add Rocky Linux Boot Option Name.
3. [Enhancements][Rome BIOS] Update Rome B0 stepping CPU microcode 0x0830107A for AMD-SB-7008 Security Bulletin to address CVE-2023-20593 issue.
4. [Enhancements][Rome BIOS] Restore SMCI secure boot keys and Update Secure Boot DB variable. (Unknown certificate "Addtrust External CA Root" is expired on May 30th 2020)
5. [Features][Naples BIOS] Add InBand OemFID support.
6. [Features][Naples BIOS] Add OutBand OemFID support.
7. [Fixes][Naples BIOS] Update OEM FID information for PRICESSO_0_DESC and PRICESSO_1_DESC.

2.5 (10/25/2022)

1. [Naples/Rome BIOS] Update DBX file to fix Secure Boot Bypass issue
2. [Rome BIOS] Update AGESA RomePI to 1.0.0.E based on 5.14_RomeCrb_0ACMK025.

3. [Rome BIOS] Update Rome B0 stepping CPU microcode 0x08301055 to patch Errata 1161, 1176, 1179, 1183, 1214, 1268, 1386, 1417.
4. [Rome BIOS] Modify Setup string naming from SMCI to Supermicro.
5. [Rome BIOS] Remove "Vendor Keys" in security page.

2.4 (12/28/2021)

1. [Enhancements][Naples/Rome BIOS] Change BIOS revision to 2.4.
2. [Enhancements][Naples BIOS] Update AGESA NaplesPI to 1.0.0.H.
3. [Enhancements][Naples BIOS] Update 8012 ZP-B2 microcode 0800126E.
4. [Enhancements][Rome BIOS] Update AGESA RomePI to 1.0.0.D.
5. [Enhancements][Rome BIOS] Update 8310 SSP-B0 microcode 8301052.
6. [Enhancements][Rome BIOS] Per AMD's suggestion, set Relaxed Ordering default to Enabled.
7. [Enhancements][Rome BIOS] Exposed Setup item "Enhanced Preferred IO Mode".

2.1c (8/28/2020)

1. Changed BIOS revision to 2.1c.
2. Fixed system with 8TB memory support.
3. Fixed CPU speed information is not correct in BIOS SETUP.

2.1b (6/9/2020)

1. Changed BIOS revision to 2.1b.
2. Disabled NVDIMM function to patch HW redundant power failure designed limitation

2.1a (05/14/2020)

1. Changed BIOS revision to 2.1a.
2. Updated AGESA RomePI to 1.0.0.7.
3. Updated 8310 SSP-B2 microcode 8301038.
4. Fixed problem of system hanging on POSTCODE 0xB2 when JPG1 is set to disabled and the VGA card is plugged in.
5. Added SMCI HDD Security feature.
6. Fixed failure of FRU0 - Manufacturer Name(PM) to sync to SMBIOS Type 3 - Manufacturer(CM).
7. Removed "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
8. Added AMD IOMMU patch code for fixing problem of NVMe devices dropping and hardware error in RHEL 7.x.
9. Fixed TCG admin password reverse bug.

2.1 (02/21/2020)

1. Changed BIOS revision to 2.1.
2. Updated AGESA RomePI to 1.0.0.5 based on 5.14_RomeCrb_0AC MK013.
3. Displayed "PCI AER Support" setup item on ACPI page.

4. Added SMC HDD Security feature.
5. Removed requirement to use Admin password for erasing TCG device.
6. Fixed issue of system hanging at post code A7h.
7. Fixed inability of SUM to change the function of NUMA Node Per Socket.
8. Fixed problem of system sometimes rebooting during legacy Windows 2019 OS installation when using Rome CPU 7502.

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. 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. Fixed problem of the xGMI speed reaching 16G after pressing “load default.”
20. Fixed problem of the default xGMI speed not being 10.6G

2.0 (8/16/2019)

1. First Release.
2. Fixed the PXE error message “No enough memory to load an image” when load FTU7.
3. Fixed the issue of AOC sensor reading.