IPMI Firmware / BIOS Release Notes Form

Product Name	**H11SSW-iN/NT (2.0)**
Release Version	**3.0**
Release Date	**07/12/2024**
Previous Version	**2.8**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**ECO #30455** **BIOS Image: BIOS_H11SSW-1B19_20240712_3.0_STDsp.bin** **Please update BIOS with attached Flash Utility in package.**
Enhancements	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. 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 SA50218_Supplement(Vulnerabilities in EDK2 NetworkPkg) ; Quarkslab sighted seven exploitable security issues in the TianoCore EDK2 NetworkPkg which AMI integrates into Aptio V. 12. Update SA50121_Supplement(TOCTOU Vulnerability) 13. Update SA50230_Supplement(Image Parser Corruption Vulnerability). 14. Disable ASPM in ACPI FACP when pcie ASPM is disabled. 15. Update SA50235_Supplement(Extended Image Parser Corruption Vulnerability) 16. Update secure boot KEK and DB (Fellow EagleStream SVN 2926). 17. Added SmcBootModeCallBack function for setup item "boot mode" to auto switch the option roms' value. 18. Update SA50221_Supplement(UsbRt SMM Vulnerability Arbitrary Code Execution). 19. Update SA50215_Supplement(Buffer Overflow Vulnerability in SmmLockBox). 20. System would reboot during flash BIOS with watchdog function enable. 21. Update SA50243_Supplement(UsbRt TOCTOU Vulnerability). 22. Fixed memory multi-bit error will report to correctable error. 23. Update AMI Modules based on 5.14_RomeCrb_0ACMK029 ; Update Rome B0 stepping CPU microcode 0x0830107B. 24. Update AMI Modules based on 5.14_RomeCrb_0ACMK030 ; Security Update for SA50221 and SA50243.
New features	N/A
Fixes	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

Release Notes from Previous Release(s)

2.8 (2023/12/14)
1. Update AGESA RomePI to 1.0.0.H based on 5.14_RomeCrb_0ACMK028.
2. Update AGESA NaplesPI to 1.0.0.L based on 5.013_NaplesCrb_0ACIJ031.
3. Update SA50216_Supplement(LogoFAIL Vulnerability).An attacker can exploit this vulnerability by flashing firmware containing a maliciously-crafted logo image and booting this system with the altered image.
On devices vulnerable to LogoFAIL, attackers can supply custom logos and thus exploit any vulnerabilities in the image parser. This weakness affects a variety of image formats including GIF, PNG, BMP and JPEG.
4. Fixed MP1(SMU) and CPU WDT uncorrectable error no event log issue.
5. Disable "Correctable/Non-Fatal error reporting enable" bits when BIOS item "PCI AER support" set Disabled.
2.7 (2023/11/15)
1. Update AGESA RomePI to 1.0.0.G based on 5.14_RomeCrb_0ACMK027.
2. Support to changing Pxe from Uefi(U)/Legacy(L) to L/U through Redfish; It can adjust setup options and priority of Pxe boot order according to Boot Flag Command.
3. Enable token ASM1061_Workaround to disable ASM1061 64-bit memory address capability.
4. [Rome][Enhancements] Make sure the memory size is not different on DC ON/OFF.
5. [Naples][Rome][Fixes] Set RDIMM\LRDIMM\3DSDIMM memory throttling trip-point @85C, according to DDR4 Spec and our thermal design guide, Confirm that "Memory Over temperature SEL" can be triggered when the DIMM temperature exceeds 85 degrees
2.6a(2023/09/28)
1. Update AGESA RomePI to 1.0.0.F.
2. Add Rocky Linux Boot Option Name.
3. Update Rome B0 stepping CPU microcode 0x0830107A for AMD-SB-7008 Security Bulletin to address CVE-2023-20593 issue.
4. Update OEM FID information for PRICESSO_0_DESC and PRICESSO_1_DESC.
5. Add InBand OemFID support.
6. Add OutBand OemFID support.
7. Restore SMCI secure boot keys and Update the Secure Boot DB variable. (Unknown certificate "Addtrust External CA Root" is expired on May 30th 2020).
2.4(12/28/2021)
1. Update AGESA NaplesPI to 1.0.0.H.
For AMD-SB-1021 Security Advisory to address CVE-2020-12954(High), CVE-2020-12961(High), CVE-2021-26331(High), CVE-2021-0116(7.9, High), CVE-2021-26335(High), CVE-2021-26315(Medium), CVE-2020-12946(Medium), CVE-2020-12951(Medium), CVE-2021-26336(Medium), CVE-2021-26337(Medium), CVE-2021-26338(Medium), CVE-2021-26320(Medium), CVE-2020-12944(Medium), CVE-2020-12988(Medium), CVE-2021-26329(Medium), CVE-2021-26330(Medium), CVE-2021-26321(Medium), CVE-2021-26323(Medium), CVE-2021-26325(Medium), CVE-2021-26326(Medium), CVE-2021-26322(Medium), CVE-2021-26327(Medium) and CVE-2021-26312(Medium)
security issues.
2. Update 8012 ZP-B2 microcode 0800126E for 7001 series CPU.
3. Update AGESA RomePI to 1.0.0.D.
For AMD-SB-1021 Security Advisory to address CVE-2020-12954(High), CVE-2020-12961(High), CVE-2021-26331(High), CVE-2021-0116(7.9, High), CVE-2021-26335(High), CVE-2021-26315(Medium), CVE-2020-12946(Medium), CVE-2020-12951(Medium), CVE-2021-26336(Medium), CVE-2021-26337(Medium), CVE-2021-26338(Medium), CVE-2021-26320(Medium), CVE-2020-12944(Medium), CVE-2020-12988(Medium), CVE-2021-26329(Medium), CVE-2021-26330(Medium), CVE-2021-26321(Medium), CVE-2021-26323(Medium), CVE-2021-26325(Medium), CVE-2021-26326(Medium), CVE-2021-26322(Medium), CVE-2021-26327(Medium) and CVE-2021-26312(Medium)
security issues.
4. Update 8310 SSP-B0 microcode 8301052 for 7002 series CPU.
5. Per AMD's suggestion, set Relaxed Ordering default to Enabled for ROME CPU.
6. Exposed Setup item "Enhanced Preferred IO Mode" for ROME CPU.
2.2 (10/08/2020)
1. [Enhancements] Change BIOS revision to 2.2.
2. [Enhancements] Update AGESA RomePI to 1.0.0.8.
3. [Enhancements] Update 8310 SSP-B0 microcode 8301038.
4. [Enhancements] Update AGESA NaplesPI to 1.0.0.D.
5. [Enhancements] Update 8012 ZP-B2 microcode 0800126C.
6. [Enhancements] Fix system will hang on POSTCODE 0xB2 when JPG1 set to disabled and plug-in the VGA card.
7. [Enhancements] Add SMCI HDD Security feature.
8. [Enhancements] Added item "Serial Port 2 Attribute" to switch UART2 as physical COM2 or BMC SOL.
1. [Fixes] Fixed Fru0 - Manufacturer Name (PM) doesn't sync. to SMBIOS Type 3 - Manufacturer (CM).
Fixed Fru0 - Product Part/Model Number (PPM) doesn't sync. to SMBIOS Type 1 - ProductName (PN).
2. [Fixes] Remove "$SMCUNHIDE$" string from "PCI AER support" setup item help string.
3. [Fixes] Add AMD IOMMU patch code for fixing NVME Devices drop and Hardware error in RH 7.x.
4. [Fixes] Fixed TCG admin password reverse bug.

2.1(02/21/2020)
1. Change BIOS revision to 2.1.
2. Update AGESA RomePI to 1.0.0.5 based on .14_RomeCrb_0ACMK013.
3. Shown "PCI AER Support" setup item in ACPI page in BIOS menu.
4. Add SMC HDD Security feature.
5. Fixed System hang post code A7h issue.

6. SUM cannot change the function of NUMA Node Per Socket.
7. Fixed system sometimes reboot during legacy Windows 2019 OS installation when used Rome CPU 7502.
8. No need to use Admin password for erasing TCG device

2.0b (12/02/2019)
1. Change BIOS revision to 2.0b.
2. Add "DRAM Scrub Time" in Memory Configuration.
3. Do not display any AMD memory error messages during the POST phase.
4. Fixed recovery function cannot work.
5. Support OOB SATA HDD information and asset information of 2 SATA controller.
6. No screen output when Boot Mode is changed to EFI.
7. Fix system will hang when installing NVidia RTX 2080/5000/6000
8. Update AGESA RomePI to 1.0.0.4 based on 5.14_RomeCrb_0ACMK012.
9. Use AMD CBS "PCIe ARI Support" item instead of "ARI Forwarding".
10. Update item string "Input the description" and "HTTP Boot One Time" to meet
11. Show 3rd IPMI version in BIOS setup.
12. Fixed the issue that "SMCI POST Screen Message" might be shown on BIOS setup menu.
13. Fixed the issue that "SMCI POST Screen Message" might be shown on POST screen during executing EFI Shell application.
14. According to each project's board ID, update SSID of AMD Host Bridge.
15. Expose riser card string in PCIe/PCI/PnP page when plug RSC_RR1U_E16 riser card on slot6.
16. Set IOMMU default as Auto (Enabled)
17. Exposed item "Preferred IO".
18. Added SATA boot name description porting.

2.0 (08/20/2019)
1. BIOS 2.0 First release.
2. A PXE error message "Not enough memory to load an image" when production loads FTU7.