IPMI Firmware / BIOS Release Notes Form

Product Name	**H11SSL-i/C/NC (2.0)**
Release Version	**3.2**
Release Date	**01/24/2025**
Previous Version	**3.1**
Update Category	**Recommend**
Dependencies	**N/A**
Important Notes	**ECO #31295** **BIOS_H11SSL-1A03_20250124_3.2_STDsp.bin** **Please update BIOS with attached Flash Utility in package.**
Enhancements	1. [Naples][Rome] Update SA50289(TianoCompress Privilege Escalation Vulnerability) to address CVE-119 2. [Naples] Update AGESA NaplesPI to 1.0.0.P based on 5.013_NaplesCrb_0ACIJ034. 3. [Rome] Update AMI Modules based on 5.14_RomeCrb_0ACMK034;Update AGESA RomePI to 1.0.0.L. 4. [Naples] Merge SA50191 code change; Exploitation in Certificate Verification in Openssl 5. [Naples] 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.
New features	**N/A**
Fixes	N/A

Release Notes from Previous Release(s)

3.1 (10/21/2024)

1. Update AGESA NaplesPI to 1.0.0.N based on 5.013_NaplesCrb_0ACIJ033.
2. Merge SA50191 code change ; Exploitation in Certificate Verification in Openssl
3. 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. Update AMI Modules based on 5.14_RomeCrb_0ACMK033.

3.0 (07/01/2024)

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.
11. 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.

12. 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

2.9 (05/14/2024)

1. Update SA50218_Supplement(Vulnerabilities in EDK2 NetworkPkg). Quarkslab sighted seven exploitable security issues in the TianoCore EDK2 NetworkPkg, which AMI integrates into Aptio V.
2. Update SA50121_Supplement(TOCTOU Vulnerability).
3. Update SA50230_Supplement(Image Parser Corruption Vulnerability).
4. Disable ASPM in ACPI FACP when pcie ASPM is disabled. ASPM should be disabled when pcie aspm is disabled.
5. Update SA50235_Supplement(Extended Image Parser Corruption Vulnerability) to address
6. Update secure boot KEK and DB (Fellow EagleStream SVN 2926).
7. Added SmcBootModeCallBack function for setup item "boot mode" to auto switch the option roms' value.
8. Enhance get VPD data routines for E710.
9. Update AMI Modules based on 5.14_RomeCrb_0ACMK029.
10. Update AMI Modules based on 5.14_RomeCrb_0ACMK030.
11. System would reboot during flash BIOS with watchdog function enable.
12. Fixed memory multi-bit error will report to correctable error.

2.8 (12/14/2023)

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 (10/20/2023)

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. [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 (10/06/2023)

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).
8. Modify Setup string naming from SMCI to Supermicro.
9. Remove "Vendor Keys" in security page.

2.4 (12/27/2021)

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.
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.
5. Per AMD's suggestion, set Relaxed Ordering default to Enabled.
6. Exposed Setup item "Enhanced Preferred IO Mode" by AMD's suggestion.

2.1 (2/21/2020)

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. There is 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.

2.0a (08/08/2019)

1. System will hang 0xB2 when installing Intel X520-SR2 which has large VPD data.
2. Correct VGA connect type in type 8.
3. Fix bug that HD Audio test of WHQL HLK with Windows Server 2019 would detect System Audio device existence to verify audio WHQL.
4. Support USB recovery of Asmedia XHCI Controller and CPU USB ports for Agesa 1.0.0.1.
5. NVDIMM function is failed.
6. The DIMM location of IPMI "Memory Device Disabled" is incorrect.
7. Fix I210 iSCSI OPROM can't be loaded when set default setting of item "Onboard LAN1 Option ROM" to iSCSI.
8. Fixed issue that boot priority will not be restored to the default setting after flashing bios.
9. Add "SMBIOS preservation" item
10. Fix the onboard I210 LAN cannot boot to PXE in production line.

2.0 (07/29/2019)

1. First release, support both AMD ROME and Naples CPU.