

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	X10DRFR(-N/NT)
Release Version	3.4 SPS: 3.1.3.72
Build Date	5/20/2021
Previous Version	3.3
Update Category	Recommended
Dependencies	None
Important Notes	None
Enhancements	1. Exposed the “IPMI STATUS” string in the IPMI setup page. 2. Updated Grantley Refresh RC IPU2021.1 (RC 278R17) to address INTEL-TA-00463: CVE-2020-12357 (7.5 High) and CVE-2020-12360 (5.6 Medium). 3. Updated Haswell-EP/Broadwell-EP CPU microcode from Intel-Restricted-2021-1-IPU-20210322_20211IPU Release.
New features	N/A
Fixes	N/A

Release Notes from Previous Release(s)

3.3 (10/24/2020)

1. Updated Haswell-EP/Broadwell-EP CPU microcode from 20201020_NDA Release.
2. Updated Grantley Refresh RC IPU2020.2 to address Intel-TA-00358: CVE-2020-0591 (6.7, Medium) and CVE-2020-0592 (3, Low), and Intel-TA-00390: CVE-2020-8738 (7.5, High), CVE-2020-8740 (6.7, Medium), and CVE-2020-8764 (8.2, High).
3. Prioritized Disk SMART error event before display of disk SMART error.

3.2 (11/20/2019)

1. Updated SINIT ACM 3.1.4 PW for Intel-SA00240 (CVE-2019-0151 CVSS 3.1: 7.5 High).
2. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.2.0.1034.
3. Updated Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B000038 for Intel-SA00219 (CVE-2019-0117) and Intel-SA00220 (CVE-2019-0123).

3.1c (4/27/2019)

1. Updated Intel Server Platform Services 3.1.3.72 for Grantley Refresh Platforms.
2. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
3. Updated VBIOS and VGA EFI Driver to 1.09.
4. Updated Haswell-EP/Broadwell-EP CPU microcode from SRV_P_273 for INTEL-SA-00233 security advisory.
5. Updated valid range of IPMI setup item VLAN ID to 1-4094.
6. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
7. Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.
8. Updated CryptoPkg 32.01 for AMI SA50066.
9. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.
10. Fixed malfunction of Windows Consistent Device Naming (CDN).
11. Fixed missing MLP sensor reading.

3.1b (4/27/2019)

1. Forced a global reset if SPI descriptor is not write-protected after BIOS flash.
2. Implemented anti-rollback for FDT Read-Only.
3. Implemented multi-line IPMI page text and string.
4. Updated CPU microcode for PC6 issue.
5. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
6. Fixed malfunction of METW if many error events are triggered within a very short time.

3.1a (6/21/2018)

1. Fixed problem of 1.10 and newer revision boards repeatedly rebooting when trying to update SPS FDT region.

3.1 (6/9/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Added support for IPMI IPV6.
3. Removed unsupported memory frequency options from setup menu.
4. Disabled Cloaking for Broadwell E5-2687W V4 CPU (W: workstation SKU).
5. Updated Broadwell-EP RC 4.4.0 release.
6. Fixed problem of Afu /O command clearing SMC SMBIOS region (\$SMC).
7. Fixed problem of SUM OOB GetSataInfo always showing "Configuration Type" as "AHCI" when setting "Configure SATA as" to "RAID" or "IDE".
8. Fixed inability to enter setup menu by pressing "DEL" key if Re-try Boot feature is enabled and there are no boot devices.
9. Set Descriptor Region of BIOS Region Write Access to "No".

3.0a (2/24/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Updated Broadwell-EP RC 4.3.0 PLR11 release.
3. Updated BIOS ACM 3.1.1 PW and SINIT ACM 3.1.1 PW.
4. Corrected POST diagnostic signOn string.
5. Added tCCD_L Relaxation item under Memory Configuration menu.
6. Added SumBbsSupportFlag into DAT file.
7. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
8. Enhanced SMC Recovery Flash Boot Block feature.
9. Fixed inability of SUM to get COM2/SOL settings from BIOS.
10. Updated Intel Server Platform Services 3.1.3.50 for Grantley Refresh Platforms.
11. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014 (RSTe SATA 4.7.0.1069 and NVMe 4.7.0.2063).
12. Fixed inability of SUM utility to get "Setup Prompt Timeout" setup item.
13. Added support for AOC-SLG3-2M2 auto-bifurcation on CPU1 SXB1 SLOT.
14. Implemented SMC Recovery Flash Boot Block feature to add the POST screen message, "The System Is Going To Reset And Then Entering To Recovery Mode Again."
15. Added support for System Firmware Progress feature.
16. Fixed problem of NVDIMM setup items appearing when optimized defaults load even without NVDIMM being installed.
17. Fixed problem of SMBIOS Type4 CPU2 current speed not showing as zero when CPU2 is not installed.
18. Fixed problem of system resetting or hanging after Watch Dog function is enabled during BIOS update.
19. Fixed problem of MWAIT being disabled on BSP only.
20. Fixed inability to get correct Memory CECC DIMM location via SD5.
21. Fixed problem of system hanging at POST 0xA9 when entering setup menu while Intel P4800X uEFI driver is loaded.
22. Updated FlashDriver module to Label 5 in order to fix inability of system to enter recovery mode when MAIN block is updated 45% and then system powers off.

