

IPMI Firmware / 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	X10DRW-E/N(T)
Release Version	3.2
Release Date	11/22/2019
Previous Version	3.1c
Update Category	Critical
Dependencies	None
Important Notes	None
Enhancements	1. Changed BIOS revision to 3.2. 2. Updated SINIT ACM 3.1.4 PW for INTEL-SA-00240 Security Advisory to address CVE-2019-0151 (7.5, High) and CVE-2019-0152 (8.2, High) security issues. 3. Updated SATA/sATA RAID OPRM/EFI driver to VROC PreOS v6.2.0.1034. 4. Updated Broadwell-EP B0/M0/R0 CPU microcode MEF406F1_0B000038 for INTEL-SA-00219 Security Advisory to address CVE-2019-0117 (6.0, Medium) security issue and for INTEL-SA-00220 Security Advisory to address CVE-2019-0123 (8.2, High) and CVE-2019-0124 (8.2, High) security issues.
New features	N/A
Fixes	N/A

Release Notes from Previous Release(s)

3.1c (05/02/2019)

1. Changed BIOS revision to 3.1c.
2. Forced a global reset if SPI descriptor is not write-protected after BIOS flash.
3. Implemented anti-rollback for FDT Read-Only.
4. Implemented multi-line IPMI page text and string.
5. Updated EIP393007 & EIP411789 for TPM vulnerability when resuming S3.
6. Updated Intel Server Platform Services 3.1.3.72 for Grantley Refresh Platforms.
7. Updated SATA/ssATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
8. Updated VBIOS and VGA EFI Driver to 1.09.
9. Updated Haswell-EP/Broadwell-EP CPU microcode from SRV_P_273 for INTEL-SA-00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127, and CVE-2018-12130 security issues.
10. Updated valid range of IPMI setup item VLAN ID to 1-4094.
11. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
12. Added support for setting IPv6 Static Router1 prefix length and value in BIOS setup menu feature.
13. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
14. Fixed malfunction of METW if many error events are triggered within a very short time.
15. Displayed the driver health support pages to support LSI (Broadcom 9440-8i) driver health status.
16. Fixed malfunction of Windows Consistent Device Naming (CDN).

3.1 (06/07/18)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS version to 3.1.
3. Updated Broadwell-EP RC 4.4.0 release.
4. Added support for IPMI IPV6.
5. Removed unsupported memory frequency options from setup menu.
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 failure of SMBIOS to change to default even if preserve SMBIOS setup item is set to disabled during recovery.
9. Set Descriptor Region of BIOS Region Write Access to "No".

3.0a (04/16/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v4.7.0.1014.
3. Updated Intel Server Platform Services 3.1.3.50 for Grantley Refresh Platforms.
4. Removed support for using Ctrl+home to trigger recovery.
5. Changed BIOS revision to 3.0a.
6. Changed Memory correctable threshold to 100 and enabled Cloaking for Broadwell CPU E5-26xx SKU.
7. Patched workaround for QPI error.