

## 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.*

<b>Product Name</b>	<b>X11SSH-G(T)F-1585(L)</b>
<b>Release Version</b>	<b>1.3</b>
<b>Release Date</b>	<b>11/26/2019</b>
<b>Previous Version</b>	<b>1.2b</b>
<b>Update Category</b>	<b>Critical</b>
<b>Dependencies</b>	<b>None</b>
<b>Important Notes</b>	<b>None</b>
<b>Enhancements</b>	<b>1. Changed BIOS revision to 1.3. 2. Updated SPS 4.01.04.088 PLR version for INTEL-SA-00241 Security Advisory to address CVE-2019-11090 (6.8, Medium), CVE-2019-11088 (7.5, High), CVE-2019-0165 (4.4, Medium), CVE-2019-0166 (5.9, Medium), CVE-2019-0168 (4.6, Medium), CVE-2019-0169 (9.6, Critical), CVE-2019-11086 (3.5, Low), CVE-2019-11087 (6.4, Medium), CVE-2019-11101 (4.4, Medium), CVE-2019-11100 (6.1, Medium), CVE-2019-11102 (4.1, Medium), CVE-2019-11103 (7.3, High), CVE-2019-11104 (7.3, High), CVE-2019-11105 (7.9, High), CVE-2019-11106 (4.4, Medium), CVE-2019-11107 (5.3, Medium), CVE-2019-11108 (2.3, Low), CVE-2019-11110 (4.1, Medium), CVE-2019-11097 (7.3, High), CVE-2019-0131 (7.1, High), CVE-2019-11109 (4.4, Medium), CVE-2019-11131 (7.5, High), CVE-2019-11132 (8.4, High), and CVE-2019-11147 (8.2, High) security issues.</b>

	<p>3. Updated SI 4.1.1.3 for INTEL-SA-00260 Security Advisory to address CVE-2019-0154 (6.5, Medium) security issue.</p> <p>4. Updated Skylake-H CPU microcode M36506E3_000000D6 for INTEL-SA-00219 Security Advisory to address CVE-2019-0117 (6.0, Medium) security issue, INTEL-SA-00289 Security Advisory to address CVE-2019-11157 (7.9, High) security issue, and INTEL-SA-00242 Security Advisory to address CVE-2019-11112 (8.8, High), CVE-2019-0155 (8.8, High), CVE-2019-11111 (7.3, High), CVE-2019-14574 (6.5, Medium), CVE-2019-14590 (6.5, Medium), CVE-2019-14591 (6.5, Medium), CVE-2019-11089 (5.9, Medium), and CVE-2019-11113 (4.0, Medium) security issues.</p> <p>5. Updated Skylake BIOS ACM 1.6.0 and SINIT ACM 1.7.4 for INTEL-SA-00220 Security Advisory to address CVE-2019-0123 (8.2, High) and CVE-2019-0124 (8.2, High) security issues and INTEL-SA-00240 Security Advisory to address CVE-2019-0151 (7.5, High) and CVE-2019-0152 (8.2, High) security issues.</p> <p>6. Updated Secure Boot Key.</p> <p>7. Implemented security update for INTEL-SA-00254 Security Advisory to address CVE-2019-0185 (6.0, Medium) security issue.</p>
New features	N/A
Fixes	N/A

**Release Notes from Previous Release(s)**

**1.2b (5/24/2019)**

1. Updated Intel CPU microcode from DT\_P\_183 for INTEL-SA00233 Security Advisory to address CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, and CVE-2019-11091 security issues.
2. Contained SPS 4.01.04.054 PLR version for security vulnerability INTEL-SA-00213 to address CVE-2019-0089, CVE-2019-0090, CVE-2019-0086, CVE-2019-0091, CVE-2019-0092, CVE-2019-0093, CVE-2019-0094, CVE-2019-0096, CVE-2019-0097, CVE-2019-0098, and CVE-2019-0099 security issues.
3. Changed BIOS revision to 1.2a.
4. Updated SATA RAID OPRM/EFI driver to RSTe PreOS v4.7.0.1017.
5. Updated VBIOS and VGA EFI Driver to 1.09 to fix ASpeed CVE-2019-6260 security issue.
6. Updated valid range of IPMI setup item VLAN ID to 1-4094.
7. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
8. Fixed inability to disable SMBIOS preservation for recovery.
9. Fixed inability to log CECC events in IPMI event log when METW = 0.

**1.2 (8/29/2018)**

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Changed BIOS revision to 1.2.
3. Updated Kaby Lake BIOS ACM 1.4.0 and SINIT ACM 1.3.0.
4. Enhanced ability to enter setup menu without password when system only has Administrator password.
5. Updated EIP419363 to ensure DCI Policy is "Disabled" for INTEL-SA-00127, EIP412144 for [SA50044] USRT Mantis vulnerabilities, and EIP387724 for Ofbd Meud Security vulnerabilities.
6. Fixed problem of Afu /O command clearing SMC SMBIOS region (\$SMC).
7. Implemented workaround for problem of IP displaying 0.0.0.0 information the first time AC powers on BMC.
8. Fixed problem of the system hanging when trying to create virtual driver on LSI3108 storage card under BIOS setup.
9. Fixed missing reminding string "iKVM doesn't support add-on VGA device..." when VGA is plugged in & "Primary Display"=="PEG".
10. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
11. Fixed missing iSCSI OPRM Ctrl+D execution when X710 iSCSI OPRM is updated to rev1861.
12. Fixed issue of UEFI Boot option becoming disabled if HDD is re-plugged in with UEFI OS.
13. Fixed inability of SMBIOS preservation for recovery to be set to disabled.

**1.1 (12/6/2017)**

1. Changed BIOS revision to 1.1.
2. Updated Skylake-S R0/S0 stepping MCU M36506E3\_000000C2.

--