IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SSH-G(T)F-1585(L)**
Release Version	**1.2**
Release Date	**8/29/2018**
Previous Version	**1.1**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**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 Skylake 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.**
New features	**N/A**
Fixes	**1. Fixed problem of Afu /O command clearing SMC SMBIOS region ($SMC).**

	2. Implemented workaround for problem of IP displaying 0.0.0.0 information the first time AC powers on BMC.
	3. Fixed problem of the system hanging when trying to create virtual driver on LSI3108 storage card under BIOS setup.
	4. Fixed missing reminding string "iKVM doesn't support add-on VGA device..." when VGA is plugged in & "Primary Display"=="PEG".
	5. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
	6. Fixed missing iSCSI OPROM Ctrl+D execution when X710 iSCSI OPROM is updated to rev1861.
	7. Fixed issue of UEFI Boot option becoming disabled if HDD is re-plugged in with UEFI OS.
	8. 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.