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	**X11DSF-E**
Release Version	**2.1**
Release Date	**8/24/2018**
Previous Version	**2.0b**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.** **2. Enabled BIOS secure flash upgrade feature (firmware signature).** **3. Corrected BIOS/ME downgrade check for SPS 4.0.4.340 and later.** **4. Displayed Memory DIMM PPR setup item.** **5. Checked PCH SKU for QAT enabled board.** **6. Added message "Secure Flash Recovery Image Verification Failed." for prompting user if secure flash recovery image is invalid.** **7. Updated SPS 4.0.4.381 for INTEL-SA-00131 Security Advisory to address CVE-2018-3643 and CVE-2018-3644 security issues.**
New features	**N/A**

Fixes	**1. Fixed failure of WDT function.** **2. Fixed inability of system to clean event log via Afu command "/CLNEVNLOG".** **3. Fixed issue with IPMI firmware to enable storage card to show temperature.**