IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPS-RE**
Release Version	**3.0a SPS : 4.1.3.239**
Release Date	**4/2/2019**
Previous Version	**2.1a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Added support for Purley Refresh platform.** **2. Updated Skylake H0/M0/U0 CPU microcode to version 57.** **3. Updated Intel® RSTe package to version 6.0.0.1024.** **4. Set NVDIMM ADR timeout to 600µs.**
New features	**1. Added ME Jumpless Recovery Feature.**
Fixes	**N/A**

2.1a (10/3/2018)

1. Updated the RSTe revision to 5.5.0.1028.
2. Enhanced the BIOS secure flash upgrade feature (firmware signature).
3. Fixed the 50-second delay when booting into UEFI shell, DOS, and various Operating Systems (OS).
4. Fixed DMI writing error with full memory DIMM and ruler NVMe SSD plugged in.

2.1 (7/18/2018)

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. Added security signature feature for IPMI BIOS Upgrade.
4. Implemented RSD feature.
5. Fixed inability of system to detect SATA device when the PCH is very hot.