MCRPS Patch Note #1: Firmware Corruption Due to Malformed Header Modification

Issue Description:

- During third party penetration testing, it was discovered during firmware update, malformed header modification led to unexpected behavior
- Patch updates the processing of file headers in the unit's firmware to avoid undefined behavior

Recommended solution:

- Download affected units' firmware package
- Verify download via hash
- Download and install security patch via MCRPS PMbus update to units

Unit	FW Package file	SHA-384 Verify Hash
CSU2400AT-3-3M0_87_87_80	CSU2400AT-3-3M0_87_87_80.bin	fb94ceb3fff1f0c393291f3fc471ed72a152cf5ab833f172afa48b13ec47ed01cd5081a0bd56d0133e5ce6ff71909932
CSU3200AT-3-3M0_67_67_80	CSU3200AT-3-3M0_67_67_80.bin	661caba2573266e77f48fff19b5e26a03cf000c6bb1e138a1fae57f5bfce32e688233b8f9366023c657812d1adf8fe05

Mitigation in place solution:

- Users should any or all of the following actions:
  - Take system level steps to ensure only properly signed firmware updates are sent to effected units
  - Compare known hashes of firmware bundles to ensure bit true representation
    - Disable BMC’s ability to update PSU firmware via commands over PMBus