Statement of Volatility – Dell EMC PowerEdge - R7415

Dell EMC PowerEdge - R7415 contains both volatile and non-volatile (NV) components. Volatile components lose their data immediately upon removal of power from the component. Non-volatile components continue to retain their data even after the power has been removed from the component. Components chosen as user-definable configuration options (those not soldered to the motherboard) are not included in the Statement of Volatility. Configuration option information (pertinent to options such as microprocessors, remote access controllers, and storage controllers) is available by component separately. The following NV components are present in the PowerEdge - R7415 server.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
Planer				
CPU Internal CMOS RAM	Non-Volatile	1	CPU0	64M bytes
BIOS SPI Flash	Non-Volatile	1	U4	256 MB
iDRAC SPI Flash	Non-Volatile	1	U5	32 MB
BMC EMMC	Non-Volatile	1	U_EMMC2	8 GB
System CPLD RAM	Volatile	1	U_CPLD1	16 KB
System Memory	Volatile	1	CPU0: A1~A16,	Up to 32GB per DIMM (RDIMM) Up to 128GB per DIMM (LRDIMM)
CPU Vcore and VDDCR SOC FW	Non-Volatile	1	PAAU1 PBAU1	16KB
MEM_VDDQ FW	Non-Volatile	1	PAEU1, PBEU1	16KB
LOM NVRAM	Non-Volatile	1	U_LOM1_ROM	8MB
Trusted Platform Module (TPM, TPM 2.0 only)	Non-Volatile	1	J_TPM_MODULE	128 Bytes
Power Supplies				
Microcontroller	Non-Volatile	Up to 2	Microchip	Up to 64KB
2U 3.5"x8 Backplane				
SEP internal flash	Non-Volatile	1	U_SEP1	Flash:32B
BP FRU image	Non-Volatile	1	U_SEP1	EEPROM: 2KB

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
2U 3.5"x12 Backplane				
NVSRAM memory	Non-Volatile	1	U_NVSRAM	MRAM: 1 Mb
Flash memory	Non-Volatile	1	U_FLASH	Flash: 128 Mb
Expander FRU image	Non-Volatile	1	U_EXP_EEPROM	512 Bytes
BP FRU image	Non-Volatile	1	U_BP_EEPROM	256 Bytes
PERC for 2U 3.5"x12 BP(H330MM)				
NVSRAM memory	Non-Volatile	1	U1033	128KB
FRU	Non-Volatile	1	U1019	256B
1-Wire EEPROM	Non-Volatile	1	U1004	128B
SBR	Non-Volatile	1	U1020	8KB
Flash	Non-Volatile	1	U3	16MB
2U 2.5x24 NVMe Backplane				
SEP internal flash	Non-Volatile	2	U_SEP1, U_SEP2	Flash: 64 Bytes
SEP internal EEPROM	Non-Volatile	2	U_SEP1, U_SEP2	EEPROM: 2K Bytes
HOTPLUG_PERST BUFFER	Non-Volatile	2	U35, U42	FRAM: 16 KB
2U 2.5x24 NVMe Expander				
PSoC	Non-Volatile	1	U_8	Flash: 128 kB
Expander FRU image	Non-Volatile	1	U_FRU	EEPROM: 2Kb
PERC for 2U 2.5"x24 BP(HBA330)				
NVSRAM memory	Non-Volatile	1	U1033	128KB
FRU	Non-Volatile	1	U1019	256B
Serial Boot ROM	Non-Volatile	1	U1020	8KB
Flash	Non-Volatile	1	U3	16MB
ACE IDSDM - vFlash				
vFlash	Non-Volatile	1	J_Ace1	Nand Flash:16GB
iDSDM	Non-Volatile	1	J_Ace1	Nand Flash :16GB,32GB,64GB

Dell - Internal Use - Confidential

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
TPM				
Trusted Platform Module (TPM, TPM 2.0 only)	Non-Volatile	1	J_TPM_MODULE	EEPROM:128 Bytes
Left (Quick Sync 2.0 module) Ear				
MCU	Non-Volatile	1	USAM7	32Mb
Left (status) Ear				
MCU	Non-Volatile	1	U_TINY	8KB
BOSS				
SPI FLASH	Non-Volatile	1	U17	1024KB
TFRU	Non-Volatile	1	U7	64KB
LCD Bezel				
Microcontroller	Non-Volatile	1	IC1	256KB
Right Ear				
SPI Flash	Non-Volatile	1	U2	32Mb

Dell - Internal Use - Confidential

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
Planer			
CPU Internal CMOS RAM	Battery-backed CMOS RAM	No	Real-time clock and BIOS configuration settings
BIOS SPI Flash	SPI Flash	Yes	Boot code, system configuration information, UEFI environment, Flash Disceptor, ME
iDRAC SPI Flash	SPI Flash	No	iDRAC Uboot (bootloader), server managent persistent store (i.e. IDRAC MAC Address, iDRAC boot variables), lifecycle log cache, virtual planar FRU and EPPID, rac log, System Event Log,
BMC EMMC	eMMC NAND Flash	No	Operational iDRAC FW, Lifecycle Controller (LC) USC partition, LC service diags, LC OS drivers, USC firmware
Memory VDDQ, CPU Vcore and VSA Regulators	OTP(one time programmable)	No	Operational parameters
System CPLD RAM	RAM	No	Not utilized
System Memory	RAM	Yes	System OS RAM
Trusted Platform Module (TPM, TPM 2.0 only)	EEPROM	Yes	Storage of encryption keys
Power Supplies			
Microcontroller	Flash PROM and EEPROM	Yes	Report PSU information and control firmware
2U 3.5"x8 Backplane			
SEP internal flash	Flash	No	FW configuration data
SEP internal flash	EEPROM	No	FRU
2U 3.5"x12 Backplane			
NVSRAM memory	MRAM	No	Configuration data
Flash memory	Flash	No	Card firmware
Expander FRU image	EEPROM	No	FRU

Dell - Internal Use - Confidential

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
BP FRU image	EEPROM	No	FRU
PERC for 2U 3.5"x12 BP(H330MM)			
NVSRAM memory	NVSRAM	No	Configuration data
FRU	FRU	No	Card manufacturing information
1-Wire EEPROM	1-Wire EEPROM	No	Holds default controller properties/settings
SBR	SBR	No	Boot loader
Flash	Flash	No	Card firmware
2U 2.5x24 NVMe Backplane			
SEP internal flash	Flash	No	FW config data
SEP internal EEPROM	EEPROM	No	FRU
HOTPLUG_PERST BUFFER	FRAM	No	Configuration data
2U 2.5x24 NVMe Expander			
PSoC	Flash	No	Configuration data
Expander FRU image	EEPROM	No	FRU
PERC for 2U 2.5"x24 BP(HBA330)			
NVSRAM memory	NVSRAM	No	Configuration data
FRU	FRU	No	Card manufacturing information
Serial Boot ROM	Serial Boot ROM	No	Boot loader
Flash	Flash	No	Card firmware
ACE IDSDM - vFlash			
vFlash (uSD)	NAND flash	Yes	Populate out-of-band or optionally connect to the host as mass storage and boot mechanism

Dell - Internal Use - Confidential

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
iDSDM (uSD1, uSD2)	NAND flash	Yes	Provides mass storage
TPM			
Trusted Platform Module (TPM, TPM 2.0 only)	EEPROM	Yes	Storage of encryption keys
Left (Quick Sync 2.0 module) Ear			
MCU	embedded Flash	No	Card firmware
Left (status) Ear			
MCU	embedded Flash	No	Card firmware
BOSS			
SPI Flash	FLASH EEPROM	No	Boot code, FW
TFRU	FLASH EEPROM	Yes	Thermal monitoring
LCD Bezel			
Microcontroller	Internal Flash	No	Boot loader and s/w implementation of LCD command set
Right Ear			
SPI Flash	SPI Flash	No	For field maintenance. Have License, Service Tag and system information.

Dell - Internal Use - Confidential

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
Planer			
CPU Internal CMOS RAM	BIOS	N/A – BIOS only control	1) Set NVRAM_CLR jumper to clear BIOS configuration settings at boot and reboot system. 2) Power off the system, remove coin cell battery for 30 seconds, replace battery and then power back on. 3) Restore default configuration in F2 system setup menu.
BIOS SPI Flash	SPI interface via iDRAC	Software write protected	Not possible with any utilities or applications and system is not functional if corrupted or removed.
iDRAC SPI Flash	SPI interface via iDRAC	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed.	The user cannot clear memory completely. However, user data, lifecycle log and archive, SEL, and fw image repository can be cleared using Delete Configuration and Retire System, which can be accessed through the Lifecycle Controller interface.
BMC EMMC	NAND Flash interface via iDRAC	Embedded FW write protected	The user cannot clear memory completely. However, user data, lifecycle log and archive, SEL, and fw image repository can be cleared using Delete Configuration and Retire System, which can be accessed through the Lifecycle Controller interface.
Memory VDDQ, CPU Vcore and VSA Regulators	Once values are loaded into register space a cmd writes to nvm.	There are passwords for different sections of the register space	The user cannot clear memory.
System CPLD RAM	Not utilized	Not accessible	Not accessible
System Memory	System OS	System OS	Reboot or power down system
Trusted Platform Module (TPM, TPM 2.0 only)	Using TPM Enabled operating systems	SW write protected	F2 Setup option
Power Supplies			
Microcontroller	The data is flash via Dell Update Package(DUP)	Using signature and manufacture key to protect memory write	Before firmware update, the memory will be clear.

Dell - Internal Use - Confidential

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
2U 3.5"x8 Backplane			
SEP internal flash	Pre-programmed before assembly	Not WP	The user cannot clear memory.
SEP internal flash	Programmed at ICT during production.	Not WP	The user cannot clear memory.
2U 3.5"x12 Backplane			
NVSRAM memory	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
Flash memory	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
Expander FRU image	Programmed at ICT during production.	Not WP	The user cannot clear memory.
BP FRU image	Programmed at ICT during production.	Not WP	The user cannot clear memory.
PERC for 2U 3.5"x12 BP(H330MM)			
NVSRAM memory	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
FRU	Programmed at ICT during production.	Not WP	Cannot be cleared with existing tools available to the customer
1-Wire EEPROM	ROC writes data to this memory	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
SBR	Pre-programmed before assembly	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
2U 2.5x24 NVMe Backplane			
SEP internal flash	Pre-programmed before assembly	Not WP	Not user clearable
SEP internal EEPROM	Programmed at ICT during production.	Not WP	Not user clearable
HOTPLUG_PERST BUFFER	Programmed at ICT during production.	Not WP	Not user clearable
2U 2.5x24 NVMe Expander			
PSoC	Pre-programmed before assembly. Can be updated using Dell/Cypress tools	Not WP. Not visible to Host Processor	Cannot be cleared with existing tools available to the customer
Expander FRU image	Programmed at ICT during production.	Not WP	Not user clearable
PERC for 2U 2.5"x24 BP(HBA330)			

Dell - Internal Use - Confidential

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
NVSRAM memory	ROC writes configuration data to NVSRAM	No write protect. Not visible to Host Processor	The user cannot clear memory.
FRU	Programmed at ICT during production	No write protect	The user cannot clear memory.
Serial Boot ROM	Pre-programmed before assembly	No write protect. Not visible to Host Processor	The user cannot clear memory.
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	No write protect. Not visible to Host Processor	The user cannot clear memory.
ACE IDSDM - vFlash			
vFlash (uSD)	User can provide data to iDRAC (entirely in the iDRAC domain) to be pushed into vFlash	No write protect	1. The card may be physically removed and destroyed or cleared via standard means on a separate computer. Or 2. The user has access to the card in the host domain and may clear it manually.
iDSDM (uSD1, uSD2)	Device resides in host domain; they are exposed to the user via an internally connected, non-removable USB mass storage device	Physical write protect switch on ACE card	(1) card may be physically removed and destroyed or cleared via standard means on a separate computer OR (2)User has access to the card in the host domain and may clear it manually
TPM			
vFlash (uSD)	User can provide data to iDRAC (entirely in the iDRAC domain) to be pushed into vFlash	No write protect	1. The card may be physically removed and destroyed or cleared via standard means on a separate computer. Or 2. The user has access to the card in the host domain and may clear it manually.
Left (Quick Sync 2.0 module) Ear			
MCU	Pre-programmed before assembly	N/A	The user cannot clear memory.
Left (status) Ear			
MCU	Pre-programmed before assembly	N/A	The user cannot clear memory.
BOSS			
SPI Flash	By programming the image via firmware update process	N/A	Use Flash tool, type “go.nsh w y”
TFRU	During Manufacturing, by programming the image via firmware update process. During runtime, by I2C Proprietary Command Protocol	N/A	By writing to Flash
LCD Bezel			

Dell - Internal Use - Confidential

Item	How is data input to this memory?	How is this memory write protected?	How is the memory cleared?
Microcontroller	Updated as part of secure iDRAC software update. Configuration parameters can change only as part of iDRAC update	Writes are only allowed as part of secure iDRAC update	not user clearable.
Right Ear			
SPI Flash	SPI interface via iDRAC	Hardware strapping	The user cannot clear memory.

NOTE: For any information that you may need, direct your questions to your Dell Marketing contact.

Dell - Internal Use - Confidential