Statement of Volatility–Dell EMC PowerEdge XE8545

Dell EMC PowerEdge XE8545 contains both volatile and non-volatile (NV) components. Volatilecomponents 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 XE8545 server.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
Planar				
BIOS Password (part of CPU internal CMOS RAM)	Non-Volatile	1	U24	16 bytes (out of 256 bytes used for CPU Internal CMOS RAM)
Primary BIOS SPI Flash	Non-Volatile	1	U514	32 MB
iDRAC SPI Flash	Non-Volatile	1	U217	4 MB
BMC EMMC	Non-Volatile	1	U515	8 GB
CPU VDDCR Regulators	Non-Volatile	2	U477, U480	NA
CPU VSOC Regulators	Non-Volatile	2	U481, U482	NA
CPU Vmem Regulators	Non-Volatile	4	U471, U479, U475, U476	NA
System CPLD RAM	Volatile	1	U_CPLD	240Kb
System CPLD FLASH	Non-Volatile	1	U_CPLD	256Kb
System Memory: RDIMM and LRDIMM	Volatile	Up to 16 per CPU	CPU<2:1>_CH<H:A>_D<1:0>	Up to 256GB per DIMM
Internal USB Key	Non-Volatile	1	Internal USB board	Varies
CPU	Volatile	1 or 2	U24 / U15	Various
iDRAC DDR	Volatile	1	U_IDRAC9_DRAM1	512Mb
iDRAC	Volatile	1	U_IDRAC	For CPU: 128KB + Registers Co-proc:64Kb + Registers
Recovery BIOS SPI	Non-Volatile	1	U514	32MB
10 x 2.5" Universal SAS/SATA/NVMe Backplane				
SEP internal flash	Non-Volatile	1	U_14	4Mbit in-chip SPI Serial Flash
Backplane FRU	Non-Volatile	1	U_14	256 Bytes

Item	Non-Volatileor Volatile	Quantity	Reference Designator	Size
H745 Adapter PERC				
NVSRAM	Non-volatile	1	U1087	128KB
FRU	Non-volatile	1	U1019	256B
SPD	Non-volatile	1	U22	256B
Flash	Non-volatile	1	U1086	16MB
Backup Flash	Non-volatile	1	U1100	8GB
SDRAM	Volatile	9	U1077-U1085	4GB
CPLD	Non-Volatile	1	U1088	64kb
BMU	Non-Volatile	1	U1090	180kB
Left Status CP				
Microcontroller	Non-Volatile	1	U_TINY	8KB
TPM				
Trusted Platform Module (TPM)	Non-Volatile	1	U2	128 Bytes
Right FIO 1U Package 1				
SPI Flash	Non-Volatile	1	U2	32 Mb
BOSS				
SPI FLASH	Non-Volatile	1	U17	8MB
FRU	Non-Volatile	1	U_BOSS_EEPROM1	2K
LCD Bezel				
Microcontroller	Non-Volatile	1	IC1	256KB
PSU				
DELTA 2400W PSU				
MCU	Non-volatile	2	IC805, IC703	64KB
EEPROM	Non-volatile	1	IC601	2KB
ARTESYN 2400W PSU				
Primary MCU	Non-volatile	1	U317	64KB
Secondary MCU	Non-volatile	1	U315	128KB
DCDC MCU	Non-volatile	1	U301	32KB

Item	Non-Volatileor Volatile	Quantity	Reference Designator	Size
LOM				
SPI FLASH	Non-volatile	1	U_LOM	8MB
R1A				
MCU	Non-volatile	1	U1	8kB
R2C				
MCU	Non-volatile	1	U901	8kB
R3D				
MCU	Non-volatile	1	U901	8kB
R4A				
MCU	Non-volatile	1	U1	8kB
R4B				
MCU	Non-volatile	1	U1	8kB
STD/LC RIO				
MCU	Non-volatile	1/1	U6	8kB
PDB				
CPLD RAM	Volatile	1	U_CPLD1	240Kb
CPLD FLASH	Non-volatile	1	U_CPLD1	256Kb
HSC	Non-volatile	1	PU2	256 Bytes

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)
Planar			
BIOS Password (part of CPU internal CMOS RAM)	Battery-backed CMOS RAM	Yes	Password to change BIOS settings
Primary BIOS SPI Flash	SPI Flash	No	Boot code
iDRAC SPI Flash	SPI Flash	No	iDRAC Uboot (bootloader)
BMC EMMC	eMMC NAND Flash	No	Operational iDRAC FW, Lifecycle Controller (LC) USC partition, LC service diags, LC OS drivers, USC firmware
CPU VDDCR Regulators	ROM	No	Operational parameters
CPU VSOC Regulators	ROM	No	Operational parameters
CPU Vmem Regulators	ROM	No	Operational parameters
System CPLD RAM	FLASH	No	Not utilized
System CPLD FLASH	RAM	No	Power on System Firmware
System Memory: RDIMM and LRDIMM	DRAM	Yes	System OS RAM
Internal USB Key	Flash	Yes	General purpose USB key drive
CPU	Cache + registers	Yes	Processor cache + registers
iDRAC DDR	DRAM	No	iDRAC local memory
iDRAC	Cache + registers	No	Processor cache + registers
Recovery BIOS SPI	SPI Flash	No	Recovery image
10 x 2.5" Universal SAS/SATA/NVMe Backplane			
SEP internal flash	Integrated Flash+EEPROM	No	Firmware + FRU
Backplane FRU	I2C EEPROM	No	FRU
H745 Adapter PERC			
NVSRAM	NVSRAM	No	Configuration data
FRU	EEPROM	No	Card manufacturing information
SPD	EEPROM	No	Memory configuration data
Flash	Flash	No	Card firmware
Backup Flash	Backup Flash	No	Holds cache data during power loss

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)
SDRAM	SDRAM	No	Cache for HDD I/O
CPLD	Flash	No	Power sequencing and Cache Offload
Left Status CP			
Microcontroller	Flash	No	Driving Health and Status LED
TPM			
Trusted Platform Module (TPM)	EEPROM	Yes	Storage of encryption keys
Right FIO 1U Package 1			
SPI Flash	SPI Flash	No	EasyRestore functionality: contains Service Tag, Copy of SEL logs
BOSS			
SPI FLASH	FLASH EEPROM	No	Boot code, FW
FRU	FLASH EEPROM	No	Card manufacturing information
LCD Bezel			
Microcontroller	Internal Flash	No	Bootloader and s/w implementation of LCD command set
PSU			
MCU	Internal Flash	Yes	Boot code, FW
FRU	EEPROM	No	PSU information
LOM			
SPI FLASH	SPI Flash EEPROM	Yes	Firmware
R1A			
MCU	Flash ROM	No	Riser information
R2C			
MCU	Flash ROM	No	Riser information
R3D			
MCU	Flash ROM	No	Riser information
R4A			
MCU	Flash ROM	No	Riser information
R4B			
MCU	Flash ROM	No	Riser information

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)
STD/LC RIO			
MCU	Flash ROM	No	Rear IO information
PDB			
CPLD	FPGA	No	HSC, PSU and FAN control
HSC	EEPROM	No	HSC control base setting

Item	How is data input to this memory?	How is this memory write protected?
Planar		
BIOS Password (part of CPU internal CMOS RAM)	Keyboard	N/A – BIOS only control
Primary BIOS SPI Flash	SPI interface via CPU	Software write protected
iDRAC SPI Flash	SPI interface via iDRAC	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed.
BMC EMMC	NAND Flash interface via iDRAC	Embedded FW write protected
CPU VDDCR Regulators	Programmed at factory via I2C	No write protect
CPU VSOC Regulators	Programmed at factory via I2C	No write protect
CPU Vmem Regulators	Programmed at factory via I2C	No write protect
System CPLD RAM	Not utilized	Not accessible
System CPLD FLASH	Firmware update	BIOS Security Protocols
System Memory: RDIMM and LRDIMM	System OS	OS Control
Internal USB Key	USB interface via CPU. Accessed via system OS	No write protect
CPU	Various	Various
iDRAC DDR	iDRAC Firmware	No write protect
iDRAC	iDRAC Firmware	No write protect
Recovery BIOS SPI	SPI interface via iDRAC	No write protect
10 x 2.5" Universal SAS/SATA/NVMe Backplane		
SEP internal flash	I2C interface via iDRAC	Program write protect bit
Backplane External FRU	Programmed at ICT during production.	No write protect
H745 Adapter PERC		
NVSRAM	ROC writes configuration data to NVSRAM	no write protect. Not visible to Host Processor
FRU	Programmed at ICT during production.	no write protect
SPD	Pre-programmed before assembly	no write protect. Not visible to Host Processor
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	no write protect. Not visible to Host Processor
Backup Flash	FPGA backs up DDR data to this device in case of a power failure	no write protect. Not visible to Host Processor
SDRAM	ROC writes to this memory - using it as cache for data IO to HDDs	no write protect. Not visible to Host Processor

Item	How is data input to this memory?	How is this memory write protected?
Left Status CP		
Microcontroller	I2C via iDRAC	Hardware strapping
TPM		
Trusted Platform Module (TPM)	Using TPM Enabled operating systems	SW write protected
Right FIO 1U Package 1		
SPI Flash	SPI interface from iDRAC to Right Control Panel	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed.
BOSS		
SPI FLASH	By programming the image via firmware update process	N/A
TFRU	During Manufacturing, by programming the image via firmware update process.	N/A
	During runtime, by I2C Proprietary Command Protocol	
LCD Bezel		
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
PSU		
MCU	The data is flash via Dell Update Package(DUP)	SW write protected
FRU	During Manufacturing, by programming the image via firmware update process	SW write protected
LOM		
SPI FLASH	The data is flash via Dell Update Package(DUP)	Reserving write protection function for HW design.
R1A		
MCU	The data is flash via iDRAC auto update	No write protect. Not visible to Host Processor

Item	How is data input to this memory?	How is this memory write protected?
R2C		
MCU	The data is flash via iDRAC auto update	No write protect. Not visible to Host Processor
R3D		
MCU	The data is flash via iDRAC auto update	No write protect. Not visible to Host Processor
R4A		
MCU	The data is flash via iDRAC auto update	No write protect. Not visible to Host Processor
R4B		
MCU	The data is flash via iDRAC auto update	No write protect. Not visible to Host Processor
STD/LC RIO		
MCU	The data is flash via iDRAC auto update	No write protect. Not visible to Host Processor
PDB		
CPLD	Through iDRAC	No write protect.
HSC	Programmed at ICT during production.	No write protect.

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