Dell iDRAC Response to CVE (Common Vulnerabilities and Exposures) ID CVE-2016-5685 [16 November 2016]

Summary
An authenticated user could gain Bash shell access through a string injection.

Dell Response
Dell recommends updating to the latest iDRAC firmware, which remediates this potential vulnerability.

- iDRAC8 – upgrade to version 2.40.40.40 or higher (released Oct CY2016)
- iDRAC7 – upgrade to version 2.40.40.40 or higher (released Oct CY2016)
- iDRAC6 – not affected

Dell would like to thank and credit Stan Ayzenberg for advising Dell regarding this potential vulnerability.

Dell Best Practices regarding iDRAC
Dell iDRAC's are intended to be on a separate management network; they are not designed nor intended to be placed on or connected directly to the internet. Doing so could expose the connected system to security and other risks for which Dell is not responsible.

Dell recommends using the Dedicated Gigabit Ethernet port available on rack and tower servers (additional hardware may be required). This interface is not shared with the host operating system and routes the management traffic to a separate physical network, enabling it to be separated from the application traffic. This option implies that iDRAC's dedicated network port routes its traffic separately from the server's LOM or NIC ports. About managing network traffic, the Dedicated option allows iDRAC to be assigned an IP address from the same subnet or different subnet in comparison to the IP addresses assigned to the Host LOM or NICs.

Along with locating DRACs on a separate management subnet, users should isolate the management subnet/vLAN with technologies such as firewalls, and limit access to the subnet/vLAN to authorized server administrators.