Dell EMC iDRAC Response to CVE (Common Vulnerabilities and Exposures) ID CVE-2016-2183 [15 May 2017]

TECHNICAL SUMMARY

The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.

Dell Response
Dell is in the process of removing DES and 3DES ciphers permanently from iDRAC7/8 on port 443 and port 5900. This will be reflected in future releases.

With current releases, customers can disable DES and 3DES ciphers on port 443 by configuring SSL Encryption strength to “256 bit or higher”.

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

Along with locating iDRACs 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.

Dell recommends upgrading to the latest version of iDRAC firmware.