Dell EMC iDRAC Response to Common Vulnerabilities and Exposures (CVE) CVE-2017-1000251 “BlueBorne” [26 Sept 2017]

OVERVIEW

The following is the Dell EMC response to the recent CVE related to the BlueBorne vulnerability.

TECHNICAL SUMMARY

The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 3.3-rc1 and up to and including 4.13.1, have been reported to be vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.

Dell EMC Response

The above CVE is not applicable to iDRAC given its design and intended use. The iDRAC9 Quick Sync 2 solution uses Bluetooth Low Energy (BLE) and disables Bluetooth classic connections. CVE-2017-1000251 is applicable to Bluetooth classic implementations.

The following table shows the various iDRAC firmware versions by server generation and the Dell EMC response.

iDRAC	iDRAC firmware version	Target Release date	Dell EMC Response
iDRAC9	3.00.00.00 or higher	N/A	Not Affected (uses BLE only)
iDRAC8	Any	N/A	Does not use Bluetooth
iDRAC7	Any	N/A	Does not use Bluetooth
iDRAC6	Any	N/A	Does not use Bluetooth

Dell EMC Best Practices regarding iDRAC

In addition to maintaining up to date iDRAC firmware and disabling lower protocols in your browser, Dell EMC also advises the following:

- iDRACs are not designed nor intended to be placed on or connected to the internet; they are intended to be on a separate management network. Placing or connecting iDRACs directly to the internet could expose the connected system to security and other risks for which Dell EMC 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.