Dell OpenManage Response to CVE (Common Vulnerabilities and Exposures) ID CVE-2016-0800, CVE-2016-0703 and CVE-2016-0704 [03 March 2016]

Overview

This is a response to the following CVE's - CVE-2016-0800 (a.k.a. DROWN), CVE-2016-0703 and CVE-2016-0704.

Summary

A cross-protocol attack was discovered that could lead to decryption of TLS sessions by using a server supporting SSLv2 and EXPORT cipher suites as a Bleichenbacher RSA padding oracle. Note that traffic between clients and non-vulnerable servers can be decrypted provided another server supporting SSLv2 and EXPORT ciphers (even with a different protocol such as SMTP, IMAP or POP) shares the RSA keys of the non-vulnerable server. This vulnerability is known as DROWN (CVE-2016-0800 - *Cross-protocol attack on TLS using SSLv2*). Similarly with CVE-2016-0703 - *Divide-and-conquer session key recovery in SSLv2* leads to a more efficient version of DROWN that is effective against non-export cipher suites, and requires no significant computation. Additionally with CVE-2016-0704 - *Bleichenbacher oracle in SSLv2* could potentially allow more efficient variants of the DROWN attack.

Dell Response

All Dell OpenManage products have disabled the SSLv2 and SSLv3 protocols as a response to previously reported vulnerabilities such CVE-2015-3197 and CVE-2014-3566 (aka POODLE). As such the products are not vulnerable to the above listed issues.

Unaffected products include:

PRODUCT	VERSIONS
iDRAC6 with Lifecycle Controller	All
iDRAC7 with Lifecycle Controller	All
iDRAC8 with Lifecycle Controller	All
Chassis Management Controller (CMC)	All
Baseboard Management Controller (BMC)	All
OpenManage Integration with VMware vCenter	All
Dell Lifecycle Controller Integration (DLCI) for Microsoft System Center Virtual Machine Manager (SCVMM)	All
Dell Tool Kit (DTK)	All

Dell iDRAC Service Module (iSM)	All
Dell Connectors for CA/IBM/HP	All
Dell Plug-in for Oracle Enterprise Manager	All
Dell OpenManage Server Administrator (OMSA)	All
Dell OpenManage Power Center (OMPC)	All
Dell OpenManage Mobile (OMM)	All
Dell OpenManage Essentials (OME)	All
Dell Repository Manager	All
Dell YUM Repository	All
Dell Update Package (DUP)	All
Dell System Build and Update Utility (SBUU)	All

Dell Best Practices regarding iDRAC

iDRACs 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.