Dell iDRAC Response to CVE (Common Vulnerabilities and Exposures) ID CVE-2015-7270, 7271, 7272, 7273, 7274, and 7275 [02 December 2015]

Overview

Several potential security vulnerabilities have been filed and addressed as follows. Dell would like to thank and credit Google Infrastructure Security Assurance for advising Dell regarding these potential vulnerabilities.

Issues and Dell Response

CVE Number	CVE Description	Versions affected	Release Version & Target Fix Date - iDRAC7/8	Release Version & Target Fix Date - iDRAC6
CVE-2015-7270	Dell integrated Remote Access Controller (iDRAC) is subject to directory traversal issues which can allow local user authentication to be bypassed.	iDRAC6 iDRAC7 iDRAC8	2.21.21.21; released 09 Nov 2015	2.80; released 01 Dec 2015
CVE-2015-7271	Dell integrated Remote Access Controller (iDRAC) - 'racadm getsystinfo' command exposes a format string vulnerability.	iDRAC7 iDRAC8	2.21.21.21; released 09 Nov 2015	N/A
CVE-2015-7272	Dell integrated Remote Access Controller (iDRAC) - SSH interface appears to have an issue when authenticating with usernames greater than 62 character	iDRAC6	N/A	2.80; Released 01 Dec 2015
CVE-2015-7272	Dell integrated Remote Access Controller (iDRAC) - SSH restricted shell can accept input that may lead to buffer overflows.	iDRAC7 iDRAC8	2.21.21.21; released 09 Nov 2015	N/A
CVE-2015-7273	Dell integrated Remote Access Controller (iDRAC) - Repository update feature supports XML External Entity (XXE).	iDRAC7 iDRAC8	2.21.21.21; released 09 Nov 2015	N/A
CVE-2015-7274	Dell integrated Remote Access Controller (iDRAC) allows authenticated users to execute administrator privilege HTTP commands.	iDRAC6	N/A	2.80; Released 01 Dec 2015
CVE-2015-7275	Dell integrated Remote Access Controller (iDRAC) - Administrators have a limited	iDRAC6 iDRAC7 iDRAC8	2.30.30.30; Target Q1 CY2016	2.85; Target date Q1 CY2016

	potential to leverage Cross Site Scripting (XSS) in the web-browser.			

Dell Best Practices regarding iDRAC

DRACs 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 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.