Dell response to CVE (Common Vulnerabilities and Exposures) ID's

Overview

This document addresses concerns raised and noted by CVE team.

CVE-2013-4783 The Dell iDRAC 6 BMC implementation allows remote attackers to bypass authentication and execute arbitrary IPMI commands by using cipher suite 0 (aka cipher zero) and an arbitrary password.

CVE-2013-4785 iDRAC 6 firmware 1.7, and possibly other versions, allows remote attackers to modify the CLP interface for arbitrary users and possibly have other impact via a request to an unspecified form that is accessible from testurls.html.

Background

IPMI is an industry standard protocol, developed by Intel and supported by over two hundred vendors, such as Dell, HP, IBM, Cisco, NEC, and Supermicro. All major vendors support the latest version of IPMI, version 2.0, which was released in 2004. For more information on IPMI, visit Intel's website at http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-home.html

Dell and IPMI, BMC, and DRAC security

- The BMC is an out of band interface found on Dell PowerEdge servers to provide remote access. DRAC uses the same hardware as the BMC, but provides additional features as well as additional security options.
- **DRAC'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.
- Dell recommends following the best practices:
    - 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.
    - IPMI over LAN is disabled by default on all Dell 8th, 9th, 10th, 11th, and on our currently shipping 12th generation PowerEdge Servers.
    - Dell agrees with the US-CERT in regards to general connectivity – "It is important to restrict IPMI access to specific management IP addresses within an organization and preferably separated into a separate LAN segment." Dell security best practices and white papers advise against connecting DRAC to the internet.

Dell updates to items called out in the Certs

"cipher 0" is an option enabled by default on many IPMI enabled devices that allows authentication to be bypassed.

- While Cipher 0 (or any ciphers) can be enabled/disabled via IPMI commands, **Dell ships cipher 0 disabled by default**, and recommends keeping Cipher 0 disabled, whether the server is running internally or not.
- In the IPMI spec, user id 1 is to support anonymous logins. However, DRAC does not allow anonymous logins. DRAC has user id 1 always disabled with no option to enable it.
- While the IPMI spec allows for NULL passwords, DRAC does not support enabling of a user account with NULL password.

Follow manufacturer recommendations for sanitizing passwords. If none exists, destroy the flash chip, motherboard, or other areas the IPMI password may be stored.

- Passwords are stored encrypted on 8th, 9th, 10th, 11th, and 12th generation PowerEdge servers.
- Wiping the BMC – Dell offers an option for 11th and 12th generation servers with Lifecycle Controller for "deleting configuration and resetting defaults" and details on this can be found in the Lifecycle Controller User Guide.
- Other options to reset defaults, which applies to Dell's 8th, 9th, and 10th generation PowerEdge servers, is to invoke the BMC option ROM during BIOS POST (Ctrl-E), and executing the "reset to defaults" option, which will reset all users and passwords.
- Customers who use Dell's command line interface RACADM can issue the command "racadm racresetcfg" to achieve the same reset to defaults for DRAC5, iDRAC6, and iDRAC7.