Dell EMC iDRAC Response to Vulnerabilities Described in CVE-2018-1249, CVE-2018-1244, CVE-2018-1212, CVE-2018-1243 [updated 20 Sept 2018]

OVERVIEW

The following is Dell EMC's response to multiple CVEs in Integrated Dell Remote Access Controller (iDRAC). iDRAC firmware versions listed below contain fixes for these security vulnerabilities that could potentially be exploited by malicious users to compromise the affected system.

CVE Identifiers: CVE-2018-1249 (Medium), CVE-2018-1244 (High), CVE-2018-1212 (High), CVE-2018-1243 (High)

TECHNICAL SUMMARY

- **CVE-2018-1249**: Dell EMC iDRAC9 versions prior to 3.21.21.21 did not enforce the use of TLS/SSL for a connection to iDRAC web server for certain URLs. A man-in-the-middle attacker could use this vulnerability to strip the SSL/TLS protection from a connection between a client and a server.
- **CVE-2018-1244**: Dell EMC iDRAC7/iDRAC8, versions prior to 2.60.60.60, and iDRAC9 versions prior to 3.21.21.21 contain a command injection vulnerability in the SNMP agent. A remote authenticated malicious iDRAC user with configuration privileges could potentially exploit this vulnerability to execute arbitrary commands on the iDRAC where SNMP alerting is enabled.
- **CVE-2018-1212**: The web-based diagnostics console in Dell EMC iDRAC6 (Monolithic versions prior to 2.91 and Modular all versions) contains a command injection vulnerability. A remote authenticated malicious iDRAC user with access to the diagnostics console could potentially exploit this vulnerability to execute arbitrary commands as root on the affected iDRAC system.
- **CVE-2018-1243**: Dell EMC iDRAC6, versions prior to 2.91, iDRAC7/iDRAC8, versions prior to 2.60.60.60 and iDRAC9, versions prior to 3.21.21.21, contain a weak CGI session ID vulnerability. The sessions invoked via CGI binaries use 96-bit numeric-only session ID values, which makes it easier for remote attackers to perform brute-force session guessing attacks.

RESOLUTION

The following Dell EMC iDRAC firmware releases contain resolutions to these vulnerabilities:

- Dell EMC iDRAC6 version 2.91 for Monolithic servers (CVE-2018-1243 and CVE-2018-1212)
- Dell EMC iDRAC7/iDRAC8 version 2.60.60.60 (CVE-2018-1244 and CVE-2018-1243)
- Dell EMC iDRAC9 version 3.21.21.21 (CVE-2018-1249, CVE-2018-1244 and CVE-2018-1243)

Dell EMC recommends all customers upgrade at the earliest opportunity. Dell EMC recommends that customers take into account any deployment factors that may be relevant to their environment to assess their overall risk.

Dell EMC Best Practices regarding iDRAC

In addition to maintaining up-to-date iDRAC firmware, 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 only.

Link to remedies:

Customers can download software from the Dell Support site.
http://www.dell.com/support

Note: There is no plan to address CVE-2018-1243 and CVE-2018-1212 in iDRAC6 Modular Edition (the product is EOL). iDRAC6 Modular customers are requested to restrict access to the iDRAC web interface to trusted administrators only. The iDRAC6 web interface can also be disabled using options listed below:

- Using iDRAC GUI: iDRAC settings -> Services -> Web Server -> Enabled (Uncheck) or
- Using RACADM: racadm config -g cfgRacTuning -o cfgRacTuneWebserverEnable 0

Credits:

Dell EMC would like to thank Arseniy Sharoglazov (CVE-2018-1212) and Check Point Software Technologies Ltd. (CVE-2018-1243) for reporting these issues to us.