Dell EMC iDRAC Response to Common Vulnerabilities and Exposures CVE-2018-1207, CVE-2018-1211, and CVE-2018-1000116 [updated 26 June 2018]

OVERVIEW

The following is the Dell EMC response to multiple CVE's. 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 Identifier: CVE-2018-1207 (Critical), CVE-2018-1211 (High), CVE-2018-1000116 (High)

TECHNICAL SUMMARY

- CVE-2018-1207: Dell EMC iDRAC7/iDRAC8, versions prior to 2.52.52.52, contain CGI injection vulnerability which could be used to execute remote code. A remote unauthenticated attacker may potentially be able to use CGI variables to execute remote code.
- CVE-2018-1211: Dell EMC iDRAC7/iDRAC8, versions prior to 2.52.52.52, contain a path traversal vulnerability in its Web server's URI parser which could be used to obtain specific sensitive data without authentication. A remote unauthenticated attacker may be able to read configurations settings from the iDRAC by querying specific URI strings.
- CVE-2018-1000116: Dell EMC iDRAC7/iDRAC8, versions prior to 2.52.52.52, and iDRAC9 versions prior to 3.20.20.20 contain a heap corruption vulnerability in the NET-SNMP service (an open source component) which could be used to corrupt the heap memory. A remote unauthenticated attacker may be able to send malformed PDUs to the NET-SNMP service and trigger a heap corruption.

Note: iDRAC6 firmware is not impacted by these vulnerabilities.

Resolution:

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

- Dell EMC iDRAC7/iDRAC8 version 2.52.52.52
- Dell EMC iDRAC9 version 3.21.21.21
- **Dell EMC recommends all customers upgrade at the earliest opportunity.**

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.

- Dell EMC recommends that customers take into account any deployment factors that may be relevant to their environment to assess their overall risk.

Link to remedies:

Customers can download software from the Dell Support site.
http://www.dell.com/support/home/us/en/19/products/ser_stor_net/poweredge

Credits:
Dell EMC would like to thank Immunity Team (Immunity Inc.) for reporting these issues to us.