Dell response to Vulnerability Note VU#920038

Overview

This document addresses Vulnerability Note VU#920038.

Description

Administrative Web Interface in login page allows remote attackers to inject arbitrary web scripts or HTML via the vulnerable query string parameter .ErrorMsg

Affected Products

- iDRAC6 "monolithic" (rack and towers)
- iDRAC7 all models
- NOTE: iDRAC6 "modular" (blades) are not affected

Solution

Apply an Update

- Firmware updates will be posted to www.dell.com/support when available

Users should download the appropriate update for the version of iDRAC they have installed.

- iDRAC6 "monolithic" (rack and towers) – FW version 1.96; target release Q4CY13
- iDRAC7 all models – FW version 1.46.45; target release date mid/late September 2013
- NOTE: iDRAC6 "modular" (blades) are not affected; no update required

Additional Information

- **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.
- 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.

This response is for informational purposes only, and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.