From: all-employees-bounces@nmsu.edu [mailto:all-employees-bounces@nmsu.edu] **On Behalf Of** Norma Grijalva
Sent: Wednesday, April 09, 2014 3:00 PM
To: all-employees@nmsu.edu
Subject: Critical Information Security Update - ICT addressing Heartbleed, (Open SSL) vulnerability

To: NMSU Employees
From: Norma Grijalva
Date: April 9, 2014
Subject: **Critical Information Security Update -** ICT addressing Heartbleed, (Open SSL) vulnerability

As you may have seen in the news this morning, a major vulnerability known as Heartbleed has been uncovered in the technology (Open SSL) that encrypts most secure websites' transactions. Heartbleed allows attackers to pull information, such as usernames, passwords, bank/credit card account numbers, from secure web servers. See http://heartbleed.com/ for information about Heartbleed.

At this time, ICT is patching NMSU's central servers and checking the security of our partner service providers. ICT has received verification from our vendor partners that the MyNMSU portal and learn.nmsu.edu (Canvas) are not vulnerable. Microsoft windows servers do not use Open SSL and are not vulnerable. As a result, windows based services such as Email and Sharepoint are not affected.

ICT is working with all NMSU Information Technology professionals to ensure vulnerable systems across the institution are identified and appropriately patched.

As I have more information or recommendations on this issue as it concerns NMSU, I will send out follow up correspondence.

If you have any questions or concerns, do not hesitate to contact me at norma@nmsu.edu or John Roberts, NMSU's Chief Information Security Officer, at sysjcr@nmsu.edu.

Thank you.

--
Norma Grijalva, PhD
CIO/AVP Information Technology
Email: norma@nmsu.edu
phone: 575-646-7767