



Pay Pool Administrator Advisory

2014-7

Issue Date: April 14, 2014

Topic: Possible System Interruptions In Response to the “Heartbleed” Vulnerability Upgrade

Discussion: On April 7, 2014, the National Vulnerabilities Database released information about Common Vulnerabilities Exposure (CVE) 2014-0160, also known as the “Heartbleed” vulnerability. This vulnerability could allow the disclosure of sensitive information to an attacker through the vulnerable OpenSSL software, versions 1.0.1.

While CAS2Net does not use this software, ALTESS, our host database site, will accomplish patch installations on their HOST 4 systems known to be affected by the vulnerability described in CVE-2014-0160. These patch installations will begin today, Monday April 14, at 1500 EST. The patches will include any affected TEST, DEVELOPMENT, and PRODUCTION systems where they have identified the possible need for upgrade. Patches will be installed and systems will be rebooted between 1500 and 1700. At this time these installations are not expected to interrupt normal CAS2Net operations.

Action: Though we do not expect any CAS2Net system degradation as a result of the ALTESS patched, please inform your users that **there is a possibility of CAS2Net system interruptions during the ALTESS maintenance period, 1500-1700 EST, today, Monday April 14,** as patches are installed.

Thank you.