Date: April 30, 2014

From: Client Security Management Office
ADP Global Security Organization (GSO), Roseland NJ

Subject: OpenSSL “Heartbleed” Security Advisory

The U.S. Computer Emergency Readiness Team, a division of the Department of Homeland Security, released information about a serious vulnerability in the OpenSSL libraries. OpenSSL is frequently used as part of SSL and TLS encryption for websites (e.g., https), but can also be used for other encryption systems as well.

After a comprehensive analysis of ADP’s Internet sites worldwide, we have completed all remediation activity related to the Microsoft Internet Explorer Bug referred to as “Heartbleed.” We will also continue to assess and respond as necessary as our cyber threat management platforms are continuously updated to detect and respond to malicious activity.

Protecting our clients and their data has been, and always will be, a top priority for ADP.

Frequently Asked Questions:

Q: What actions did ADP take to determine its exposure to the Heartbleed OpenSSL vulnerability?
A: Using information from ADP’s routine and ongoing network scans, ADP immediately initiated an assessment of all external SSL sites and services across all of ADP’s global networks. Included within these sites were mail servers, web services, and application sites.

Q: How did ADP test to determine whether or not its sites and services were susceptible to the Heartbleed OpenSSL vulnerability?
A: ADP utilized a commercial and industry recognized network scanner, as well as performing its own independent internal assessment, to attempt exploit of this specific vulnerability. The script utilized was based upon a publicly available exploit kit.

Q: Did ADP find any sites susceptible to the Heartbleed OpenSSL Vulnerability?
A: ADP discovered a very small number of services that were susceptible to the Heartbleed OpenSSL vulnerability.

Q: What actions is ADP taking to address any sites or services affected by the Heartbleed OpenSSL vulnerability?
A: ADP has validated that all Payroll and Human Capital Management Services we provide to our customers globally are either not susceptible to the OpenSSL “Heartbleed” vulnerability or have been successfully remediated. Those customers potentially affected by this vulnerability are being offered the opportunity to execute a password change at their next login or are being contacted directly by their ADP support team.