HWS Information Technology Services

Title: Security Alert: 'Heart Bleed' Bug- Internet Security Vulnerability Identified

Here is what we know:
A security vulnerability was reported which could possibly expose passwords, credit card numbers and other personal information used on web sites. This vulnerability has been identified for sites using specific versions of an OpenSSL certificate. Certificates are used to encrypt network traffic and typically used on web sites that require a user to login. Use of a certificate is normally noted by a web address starting with "https://". Users interested in finding more information about this bug can go to www.heartbleed.com

Here is what we are doing:
IT Services has scanned over 500 hosts on the HWS network and only 9 were identified as 'affected' by this vulnerability. Most notable to the general campus network user would be the Large File Transfer (filetransfer.hws.edu) and Aventail VPN Tool (access.hws.edu). We are in the process of working with vendors to resolve this issue.

Many of our major services (HWS web site, PeopleSoft, Baseline and Exchange) are not affected by this bug.

Issue has also affected Campus resources that are not hosted on-site. The Canvas service (canvas.hws.edu) identified this issue and it was resolved last evening without issue.

We will continue to send updates as they come in.

Here is what you should be concerned with as a general user of the Internet
This security vulnerability affects a significant number web sites that you may go to on a regular basis (e.g. Tumblr, Amazon, Yahoo, etc). If there are sites that you log into on a regular basis, we recommend that you change your password for those sites as soon as possible.

Here is what you should be concerned with as an administrator of an on-campus system
Most notable software using OpenSSL are the open source web servers like Apache and nginx. Furthermore OpenSSL is used to protect for example email servers (SMTP, POP and IMAP protocols), chat servers (XMPP protocol), virtual private networks (SSL VPNs), network appliance and wide variety of client side software.
Administrators can use this site to test if their web site is vulnerable:
http://filippo.io/Heartbleed/

Contact: Current information about this bulletin may be found at http://www.hws.edu/itservices/bulletins.aspx. If you have any questions or concerns, please contact IT Services at helpdesk@hws.edu or call 315-781-HELP.

Type: Security Alert

Category: Informational

Distribution: hwsnetworkaccounts@hws.edu