"Heartbleed" OpenSSL Vulnerability

Names and titles:

Michele Norin, Chief Information Officer and Christian Schreiber, University Information Security Officer

Date::
April 10, 2014

Recent media coverage has raised a lot of questions about the "Heartbleed" vulnerability. Here are some quick facts to help you understand the risks, as well as how to protect yourself online.

What is "Heartbleed"?

When you visit secure websites, such as banking, shopping, and email, the communication between your computer and the web server is usually encrypted. Encryption makes it impossible for anyone else to read the sensitive information being exchanged between your computer and the web server.

On April 7, 2014 a flaw was discovered that could allow attackers to read communications going to and from certain web servers. This flaw was named "Heartbleed" and affected at least 500,000 web servers worldwide.

What is the University of Arizona doing about this?

The University's main web servers, including UAccess, UAConnect, WebAuth, and VPN are not vulnerable to Heartbleed. All college and unit IT managers have tools available to scan for internal servers that are vulnerable, and vulnerable servers are being patched as quickly as possible.

We're monitoring the situation, and we'll notify IT managers if we detect activity that requires immediate attention.

What should I do as a computer user?

First, don't panic. Although this is a serious computer vulnerability, security and IT professionals at the University and around the world are working to fix this flaw and reduce your risk. Here are some additional things you can do to protect yourself online:

- If you want to test whether a website is safe, you can use the simple testing tool at **https://www.ssllabs.com/ssltest/** [1]
- Be suspicious of any emails that ask you to change your password or provide other personal information. Phishing messages often target users based on recent news events, such as this vulnerability.

* More information about phishing can be found online at**http://security.arizona.edu/phishing** [2]

- Many experts are advising users to change their passwords. As a good practice, you should periodically change your passwords to all of your sensitive online accounts.

* Be sure to test the site first using the link above. If you reset your password on a vulnerable site, your password could still be vulnerable.

Source URL:https://uaatwork.arizona.edu/uannounce/heartbleed-openssl-vulnerability

Links
[1] https://www.ssllabs.com/ssltest/ [2] http://security.arizona.edu/phishing