Surviving Heartbleed: Best Practices for Schools and Educational Agencies for Mitigation and Recovery

What is the Heartbleed bug?

Heartbleed is not malware or a computer virus. It is a vulnerability inherent in certain versions of the popular OpenSSL security software, which secures and protects data sent over the Internet from eavesdropping. There is a bug in the software's programming code that, if exploited, could expose sensitive information. Because of the widespread use of OpenSSL in everything from secure websites (https://), Virtual Private Network (VPN) software, and smartphones/mobile devices, the impact of this bug is fairly high.

In essence, the bug affects the way in which OpenSSL handles "heartbeat" requests that can allow an attacker to peer into the memory of the targeted computer. In some cases, an attacker can exploit this vulnerability to retrieve important data, such as encryption keys, allowing for the decryption of communications or retrieval of sensitive data like passwords and portions of confidential emails.

It is highly likely that your school or educational agency will be affected in some way by this software vulnerability.

What versions of OpenSSL does Heartbleed affect?

The Heartbleed vulnerability only affects OpenSSL versions 1.0.1 through 1.0.1f, which were released in early 2012 through early 2014. Additionally, many popular operating systems, home network routers, and millions of mobile devices and smartphones were released during this time frame with the vulnerable OpenSSL included. The bug was fixed in version 1.0.1g released on April 7th of 2014.

Software patches are currently available for OpenSSL and many of the products that use the vulnerable software. OpenSSL versions 1.0.1g or later are not vulnerable. Additionally, there are plug-ins for browsers that can help individuals detect the vulnerability in the sites that they visit and even in their own web sites.

Affected versions of OpenSSL:

- **1.0.1 – 1.0.1f**

OpenSSL versions that are not affected:

- **1.0.0 branch and earlier**
- **1.0.1g and later**

What do I do now?

There are several things your school or educational agency can do immediately to mitigate the possibility of being a victim of the Heartbleed bug:

- *Inventory your systems for known vulnerable operating systems, hardware and firmware and patch those systems immediately to reduce the risk*
- *Contact third party vendors and determine how they are affected by the bug and what mitigating steps they have taken*
- *Use freely available tools to detect the vulnerability within commonly visited websites and especially those with which you exchange sensitive information*
- *Update vulnerable mobile devices with the latest security updates (be aware that it may take some time for carriers to push updates to mobile phones); Heartbleed mainly affects Android 4.1.1*
- *If software patches to correct the issue are not available, you can recompile the OpenSSL software itself using the "DOPENSSL_NO_HEARTBEATS" compile option*
- *For locally maintained machines, immediately generate new encryption keys and change all passwords for these systems*
- *For online services and personal online accounts, most affected online services have patched their systems by now, and you should change all your passwords across the board (especially for sites where you host personally identifiable information like banking and email)*

The Heartbleed vulnerability has been widely distributed in software for over two years now. Although most third party services have either already patched their systems, or were not vulnerable, there is currently no way to accurately determine if any of these systems have been exploited in the past. You should, therefore, ensure that you change your passwords and other login credentials as soon as you verify

that the systems are patched *(don't do this before verifying that they have been patched)*. This eliminates the possibility that attackers could use previously stolen credentials and return at a later date to access the account or data.

While the Heartbleed bug is a critical vulnerability that can pose a serious threat to data safety and security, it is important to keep the threat in perspective. With the disclosure of the bug and the resulting worldwide fervor over the impact, there will likely be increased use of the Heartbleed bug by attackers in the coming days and weeks. Therefore, it is much more important to focus immediate efforts on eliminating the vulnerability from your environments than to worry about what data may have been leaked in the past.

Where can I go to find more information?

The US Department of Education's Privacy Technical Assistance Center (PTAC) is a one-stop shop for questions relating to privacy and data security in education. PTAC's website contains a wide variety of technical assistance and guidance documents that are available to anyone at http://ptac.ed.gov/.

If you are unable to find the answers to your questions on the site, PTAC technical staff is available to provide live assistance to answer questions, help develop mitigation strategy, or provide insight and validation for your approach to addressing the Heartbleed vulnerability.

The number of external resources is expanding daily. As a starting point, you might want to review the additional information below:

http://heartbleed.com	
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160	- National Vulnerability Database maintained by the MITRE Corporation, which provides links to additional information
http://www.openssl.org/source/	- OpenSSL web page containing updates to patch the Heartbleed bug (upgrade to version 1.0.1g or later)
https://chrome.google.com/webstore/detail/chromebleed/eeoekjnjgppnaegdjbcafdggilajhpic?hl=en	- Chrome browser plug-in for detecting if a site is vulnerable to the Heartbleed bug
https://addons.mozilla.org/en-US/firefox/addon/heartbleed-checker/	- Mozilla Firefox browser plug-in for detecting if a site is vulnerable to the Heartbleed bug