

OET

Cyber Security Update: Heartbleed Bug

April 14, 2014

The Heartbleed Bug (Heartbleed) is a vulnerability in what is known as Open Secure Socket Layer (SSL) software. The software is designed to protect users when they attempt to use most applications. OpenSSL has been long accepted as the standard that most applications use to protect user logon passwords as well as providing secure applications such as banking websites, electronic mail, social media websites, etc.

Heartbleed takes advantage of a vulnerability within the OpenSSL software, which can be exploited to steal information that is entered through applications it uses. The result is that a hacker can capture all information that a user enters, while they interact with these applications. The attackers essentially eavesdrop on communications, steal data directly from the services and users, and impersonate those services and users.

Attackers that gain access to your user name and password will be able to logon to a number of applications, which can be used to steal information. This may include threats maintaining persistent access to your electronic mail and monitoring it. The Office of Enterprise Technology (OET) has taken a variety of steps to reduce the County's risk exposure:

- OET identified internal and external County applications that may be vulnerable to Heartbleed.
- OET is patching affected applications or upgrading to versions that are not vulnerable in order to mitigate the risks identified.
- OET is working with its vendors to validate that they have taken appropriate action to identify and mitigate this risk.

These above actions are designed to reduce the chances of usernames and passwords being compromised on applications that County employees use. The following link identifies vendors who are vulnerable to this attack, which may be used to determine how to respond to this threat. <https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=720951&SearchOrder=4>

Additionally, the following information is designed to highlight the websites that have and have not been affected by this vulnerability. OET recommends that you change your password on websites that have potential vulnerability. The following synopsis provided by the State of Arizona is meant to highlight the websites that are and are not vulnerable, including the status of their mitigation state.

What can I do about the Heartbleed?

All you can really do about Heartbleed is to change your password. It is suggested that you wait to change your password until you hear that the specific website has fixed the vulnerability. Otherwise you could very well be handing over your password to an undetected attacker.

By now, most sites that were vulnerable to the flaw have been patched. Listed below are major websites noting the vulnerability status and any action to be taken.

What does my agency have to do?

All agencies should take the following steps immediately on web servers that you manage:

- 1) Patch all vulnerable OpenSSL systems.
- 2) Revoke and reissue certificates that use OpenSSL/TLS.
- 3) Force user password changes for all impacted accounts.

OET is in the process of patching OET supported County applications that were identified as being affected by Heartbleed. OET has no evidence of any fraudulent activity or compromise against the County.

What should I watch out for?

- 1) Get verification that a site is safe before logging into it or changing your password. That verification can be via email from the organization or contacting their customer service.
- 2) Be alert for phishing scams. OET has received reports of email related to this vulnerability attempting to lure victims to password stealing sites. DO NOT click on links in unsolicited email to change passwords. Type the URL of the organization in a browser, login, and change your password.
- 3) Monitor your financial information (credit cards and bank accounts) for the next several days to identify and report fraudulent activity.

Some good news:

The login information for your bank is most likely safe. The following financial institutions have not been affected by Heartbleed: ***Bank of America, Chase, E*Trade, Fidelity, PNC, Schwab, Scottrade, TD Ameritrade, TD Bank, U.S. Bank, and Wells Fargo.***

What Passwords Do I Need to Change Today? (This list was provided from an outside source for popular websites. While the list is deemed accurate, you should verify directly with the website for any vulnerability.)

Email providers:

Here are the ones that were vulnerable:

- **Yahoo Mail:** Was affected! But patched. You should change your password.
- **Gmail:** Was affected! But patched.
- **Google:** Was affected! But patched. Google says you do not need to, but just to be safe, you should probably change your password for the following Google services: Search, Gmail, YouTube, Wallet, Play, Apps, and App Engine. Google Chrome and Chrome OS were not affected.

And the ones that were not:

- **AOL:** Was *not* affected. You do not need to change your password.
- **Hotmail/Outlook:** Was *not* affected. You do not need to change your password.
- **Microsoft:** Was *not* affected. You do not need to change your password.

Online stores:

Here are the ones that were vulnerable:

- **Amazon Web Services (for website operators):** Was affected. If you use Elastic Load Balancing, Amazon EC2, Amazon Linux AMI, Red Hat Enterprise Linux, Ubuntu, AWS OpsWorks, AWS Elastic Beanstalk, or Amazon CloudFront, you should change your password.
- **GoDaddy:** Was affected! But patched. You should change your password.
- **USPS:** Was affected! But patched. You should change your password
- **Netflix:** Was affected! But patched. You should change your password

And the ones that were not:

- **Groupon:** Was *not* affected. You do not need to change your password.
- **Walmart:** Was *not* affected. You do not need to change your password.
- **UPS:** Was *not* affected. You do not need to change your password.
- **eBay:** Was *not* affected. You do not need to change your password.
- **Amazon:** Was *not* affected. You do not need to change your password.
- **PayPal:** Was *not* affected. You do not need to change your password.
- **Target:** Was *not* affected. You do not need to change your password.

Tax and government-related:

Here are the ones that were vulnerable:

- **Intuit (TurboTax):** Was affected! But patched. You should change your password.

And the ones that were not:

- **Healthcare.gov:** Was *not* affected. You do not need to change your password.
- **1040.com:** Was *not* affected. You do not need to change your password.
- **FileYour Taxes.com:** Was *not* affected. You do not need to change your password.
- **H&R Block:** Was *not* affected. You do not need to change your password.
- **IRS:** Was *not* affected. You do not need to change your password.

Social networks:

Here are the ones that were vulnerable:

- **Tumblr:** Was affected! But patched. You should change your password.
- **Twitter:** Unclear. Twitter is “monitoring the situation.” So wait a few more days and then change your password.
- **Facebook:** Unclear! It has “added protections”; however, you should change your password.
- **Pinterest:** Was affected! But patched. You should change your password.

- **YouTube:** Was affected! But patched. You should change your password.
- **Flickr:** Was affected! But patched. You should change your password.

And ones that were not:

- **Hulu:** Was affected! But patched. You should change your password.
- **LinkedIn:** Was *not* affected. You do not need to change your password.

Other common websites:

Here are the ones that were vulnerable:

- **Dropbox:** Was affected! But patched. You should change your password.
- **SoundCloud:** Was affected! But patched. You should change your password.
- **Wunderlist:** Was affected! But patched. You should change your password.
- **Wikipedia:** Was affected! But patched. You should change your password.
- **Bing:** Was affected! But patched. You should change your password.
- **Instagram:** Was affected! But patched. You should change your password.
- **ESPN.go.com:** Was affected! But patched. You should change your password.
- **Reddit:** Was affected! But patched. You should change your password.
- **GoDaddy:** Was affected! But patched. You should change your password.
- **Washington Post:** Was affected! But patched. You should change your password.
- **Blogspot:** Was affected! But patched. You should change your password.

And the ones that were not:

- **Apple:** Was *not* affected. You do not need to change your password.
- **Amazon:** Was *not* affected. You do not need to change your password.
- **Evernote:** Was *not* affected. You do not need to change your password.
- **Dashlane:** Was *not* affected. You do not need to change your password.
- **Capital One:** Was *not* affected. You do not need to change your password.
- **FedEx:** Was *not* affected. You do not need to change your password.
- **CBSSports:** Was *not* affected. You do not need to change your password.
- **Zillow:** Was *not* affected. You do not need to change your password.
- **CNet:** Was *not* affected. You do not need to change your password.
- **MSN:** Was *not* affected. You do not need to change your password.