Security Bulletin:
Eric Hummel, QIP Solutions
April 11, 2014
Re: Heartbleed Vulnerability

By now you have probably heard, through news media, about a significant security issue that probably will affect you. The name that has been given to it is "Heartbleed". It is a vulnerability, not a virus or malicious software, and is so widespread and important that we feel it appropriate to provide you with an explanation of the problem and how it affects you our customers and friends. Please read this and circulate it to your IT support team. The issues that Heartbleed raises are of a technical nature but have profound impact on business risk.

What it is?
Heartbleed is a software vulnerability that was accidentally incorporated into a commonly used software library more than 2 years ago. Software libraries are basic building blocks of computer software and make development easier by reusing pieces of code in many different applications. The library, called OpenSSL, is used in thousands of software applications including many of the basic elements of the World Wide Web. The affected version of OpenSSL is widespread but it is not the only library for SSL.

SSL is a protocol that establishes trust between computers. It is one of the components that keeps your passwords private when logging into servers or applications. It is based on SSL digital certificates which you can think of it as IDs card for computers. Certificates are sold by companies who have validated that the holder of the certificate is the owner of the website and not an impostor. If the certificate's secret key is known it is possible to impersonate the server and steal passwords and other sensitive and private information undetected. Heartbleed allows a remote computer (e.g. on the internet) to ask OpenSSL to send a large chunk of memory on the vulnerable machine without any authentication. This is the big problem. Under normal circumstances we assume memory is secure and is not accessible to another computer, especially one that is not authenticated. Usernames, passwords, SSL certificates, encryption keys, credit card information and PHI are all present in memory of a computer at some point. Heartbleed could make this information available to anyone who can reach the vulnerable device from the internet without any authentication. What's more, the vulnerable versions of OpenSSL do not monitor or log any of these memory transactions. This means it is impossible to know if your system has been hacked and passwords or keys have been compromised.

What specifically is affected?
At present security experts are still analyzing the extent of the problem, so any answer may change over time. Instead of using a list we urge you to use a tool discussed below to determine if a server is vulnerable. Apparently, many other devices are also vulnerable including routers, firewalls, e-mail servers, ordinary PCs and even android phones.

Here are some of the known software that you should immediately test,

- Linux servers (Redhat, Fedora, Ubuntu, Centos, Debian, etc);
- Apache and nginx webservers;

- Cisco and Juniper routers and firewalls.
- Mobile devices running Android 4.1.1

There are patches available for some these and other software. However, software vendors are scrambling to create patches for many others. These will be available in the coming week(s). It is important to have your IT team in communication with vendors of vulnerable software so that patches can be installed as soon as possible.

One bright spot in all of this bad news is that the IIS server, and many other packages from Microsoft, as well as the iOS and OSX systems from Apple do not appear to be vulnerable. However, both Microsoft and Apple systems can run software that is vulnerable, so it is important to test all applications.

One extremely important and unique class of devices for healthcare organizations are the network enabled medical instruments. These are usually built with embedded software that may be vulnerable. Each of your vendors should be contacted and the status of the devices should be checked. If they are vulnerable, consult the vendor for options. Sometimes it is not possible to make these changes in the medical device software. In these cases the device's network must be carefully examined to determine the risk of connecting an unpatched device. A security expert should be consulted to determine the best protection strategies.

What are the consequences for you?

The next few weeks should be a very busy time for all IT security personnel. There is a great deal of testing to determine if systems and software are vulnerable. The risk of abuse is very real and presents a significant risk of long term and very expensive remediation if not addressed quickly and systematically. Naturally, smaller organizations will think that they are less at risk than large ones. This is <u>not</u> the case. Automated tools are scanning your devices to look for this vulnerability right now. If it is present, then you are at risk. Here are the highest threats.

A malicious attacker can use the Heartbleed to look in memory until he finds,

1. Usernames and passwords of an administrator on a server, router, workstation or mobile device. As the administrator, he plants other malicious logic on your device and "owns" it permanently;
2. The administrative credentials for a router, firewall or other network device. He uses that access to modify access to the trusted network of the organization and all devices that are protected by it;
3. Usernames and passwords of users on a server who have other accounts using the same password on other servers or services;
4. The private key for the SSL certificate. He then uses it to decrypt all traffic to and from the server; and
5. The credentials for internal servers and medical devices that reside in the trusted network.

These are serious risks that your organization should do what it can to prevent. In addition to the damage to your patient's privacy, the cost associated with remediating after a Heartbleed incident is extremely high.

What to do about it?

1. The largest risks to organizations are the customer facing websites. These must be tested immediately.
    a. Go to **the Qualys SSL Labs page here**, type in the name of a website, and click "Submit" to assess its vulnerability to the OpenSSL Web encryption bug. This site does a comprehensive evaluation of your SSL implementation. But note that it takes a few minutes to complete. When the scan is done, you should see a notification telling you whether the site is vulnerable to Heartbleed. There is also good information about other vulnerabilities that may exist.
    b. If the Heartbleed vulnerability is found on a device **in this order**:
        i. patch the affected device immediately;
        ii. contact your SSL Certificate provider and rekey your SSL certificates;
        iii. change ALL passwords, especially administrative ones.
2. Because it is also possible that routers and firewalls are affected, it is important to test them, and to begin the process of testing each of the internal devices that might be contain the vulnerability. Again, patch, rekey and change passwords.
3. If you use cloud based eHR or other services that process ePHI, contact the administrator and determine what they are doing to protect your data. Do not assume that they have patched their systems. Even if they have, you need to change passwords as soon as possible.
4. Finally, it is appropriate that everyone change passwords as soon as the server or device is known to be free of the vulnerability. It is also extremely important to engage your staff in helping fix the problem by explaining the importance of changing passwords at the appropriate time and not using a single password for many applications. It is especially important that users have different passwords for recreational computing versus work computing.

One thing that can help mitigate the problem is a tool called an "Intrusion Protection System". This identifies traffic that might be exploiting the Heartbleed vulnerability. If you have such a system, immediately contact your provider and install the signature for Heartbleed.

Scams

When events like this become publicized, various scam begin to be circulated. Please be cautious. Unsolicited emails should be carefully checked to make sure they don't contain malicious code. Do not open zip files from unknown sources. And of course there will also be scams that purport to protect you from the vulnerability for money. Make sure that your IT support helps users with guidance on spam and scam emails.

Summary

1. Identify vulnerable devices
2. Patch each as soon as possible
3. Rekey your SSL certificate
4. Change all passwords for the device starting with administrative accounts

This is a significant event, but it is not cause for panic. It is should be treated as a "learning moment. All of the recommendations above should be incorporated into your incident management plan. With luck the job will be done when you have patched, rekeyed and changed passwords. Thank you. Good luck.