KAUFMAN | DOLOWICH

KD Alert: Heartbleed - Pervasive OpenSSL Bugs Require Both Technical And Business Mitigation

by Christopher Nucifora, Esq. and Hsiao (Mark) C. Mao, Esq.
(April 14, 2014)

The recent panic of the OpenSSL bug, "Heartbleed" (CVE-2014-0160) demonstrates the need for businesses to mitigate their risks with more than just technical solutions. In addition to seeking legal counsel, tools such as Cyber Liability Insurance should also be considered.

I. What Is Heartbleed?

OpenSSL encryption is used by large and small businesses alike. The "Open Source" community created and maintains OpenSSL, which makes it essentially free software created and maintained by volunteers. OpenSSL allows one to create security certificates of limited use, using SSL (Secure Sockets Layer, a technology for establishing an encrypted link between a web server and a browser).

As internet security certificates can be extremely expensive from a recognized certificate agency, many enterprises use some combination of OpenSSL. Some estimate that as many as two-thirds of the world-wide-web's servers use OpenSSL.

On Monday, April 7, the internet security team of Google publicly disclosed that OpenSSL contained the Heartbleed bug, sending panic through businesses and consumers alike. The bug essentially allows attackers to obtain information from a vulnerable server in 64k packets, which can be anything. The bug may be used perniciously to compromise the secret keys used to identify the service providers and encrypt the traffic. This allows attackers to eavesdrop communications, and steal data such as names, passwords, and content, directly from the services and users, and then impersonate them.

The Heartbleed bug thereby provides a built-in back-door for competent hackers to get into many "secure websites," and extract packets of information that is otherwise private for both businesses and users. One major website immediately affected was Yahoo, followed by others.

In the following days, some struggled for solutions, and others were relatively dismissive of the problem. For example, one major internet content delivery and security company announced that although it believed that one can "fish" for information using the Heartbleed bug, it "may be impossible" to retrieve the actual private SSL keys themselves. Some started saying that "Heartbleed" was not as dangerous as first thought, even issuing public challenges to hackers to obtain the private SSL key from a vulnerable testing website.

By the next day, two white-hat hackers announced and proved that they were able to obtain the private SSL key, sending the internet community back into a panic. By the weekend, most experts concluded that the problem was indeed very pervasive, and may continue to loom for months to come. The NSA also came forward, explaining that it had known of the bug for at least two-years.

For those who are affected, it is highly recommended that they continue to follow the news and related announcements in the coming months. (E.g., see: http://mobile.theverge.com/2014/4/8/5594266/how-heartbleed-broke-the-internet.)

II. Mitigating Your Technical Risks

Experts have recommended that business have their administrators perform at least the following:

- *Scan their systems to see if they may have been compromised by Heartbleed. There are a number of "Heartbleed Checker" services and sites available. But businesses should definitely have their administrators make sure that they are using a reliable source, as opposed to someone trying to exploit the crisis.*
- *Check with the services, vendors, and websites used, to see how their network administrators are dealing with the issue. If there is no affirmative press release or notice, calls should be made.*
- *A patch has been released. However, businesses should remember that both their public and private SSL keys may have been stolen. The patch will not be a complete solution where someone may have obtained the private key.*
- *It is highly recommended that businesses obtain new security certificates, after obtaining a new public and private SSL key pair.*
- *Users should also perform a sweep and securely change their passwords. As discussed above, Heartbleed can be used to steal encrypted keys and information from both servers and users alike. Not only the hosts and servers are affected.*
- *If there is any reason to believe that data may have been compromised, it should be assumed that all information may have been compromised, and seek immediate technical and legal help.*

(See e.g., https://www.schneier.com/.)

III. Mitigating Your Legal And Business Risks

Whether a business will be legally liable for a particular cyber breach involving Heartbleed will depend on the facts of each incident. For example, California law provides that businesses must notify California residents when their personal information has been acquired, or reasonably believed to have been acquired, by an unauthorized person. (Cal. Civ. Code Sections 1798.29(a) and 1798.82(a).) In addition, where the security breach may involve more than 500 California residents, the business will be required to provide very specific information regarding the breach or suspected breach to the Attorney General. (Cal. Civ. Code Sections 1798.29(e) and 1798.82(f).) Most states have similar regulations now, although the regulations amongst states differ. Businesses that provide services across different states via the web will have to make sure that they comply with the legal requirements of each state when there is a suspected breach, particularly as to the response time, notice requirements, and reporting required. Legal counsel is highly encouraged.

Many questions have surfaced regarding why and how Heartbleed came about. Others are blaming the NSA for non-disclosure of a known bug. However, many forget that the Open Source community is generally not for profit and maintained by volunteers. And if businesses intend to control their technology costs by using a combination of both paid and free technology such as OpenSSL, they should mitigate their risks with tools such as Cyber Liability Insurance. Many are still unfamiliar with such insurance, because it is relatively new in the market. However, Cyber Liability Insurance may help protect against the costs and damages of such attacks, by helping to pay for both the remediation costs, and defending against third-party lawsuits. Especially where the software is created and maintained by only a few gatekeepers – such as in the case of OpenSSL – insurance may be even more relevant in mitigating business risks.

Of course, where business owners are seeking Cyber Liability Insurance for the first time now, they should be mindful that policies will generally have a "retroactive date" provision, where cyber attacks preceding the date will not be covered. Nonetheless, as cyber attacks such as Heartbleed are expected to be pervasive even going forward, businesses would do well by consulting their insurance brokers on what can and cannot be done.