Cooley

April 9, 2014

According to reports over the past couple of days, a major vulnerability called "Heartbleed" has been discovered in a widely used Internet protocol known as Secure Sockets Layer or SSL. As you may know, SSL manifests itself at the end user level as the little padlock at the bottom of your screen that indicates a secure connection between your computer and the remote web server. From a corporate perspective, SSL is often used to protect communications between Internet-facing corporate servers.

Reports have varied significantly in terms of the extent of the problem and the potential effects. Some reports have estimated as many as 75 percent of Internet servers may be affected. Further, some commentators have said that any sensitive information shared over an SSL connection are at risk while others have explained that any exploitation of this vulnerability would require a very narrow set of circumstances. Here is our take on the problem, along with a few steps you may want to consider depending on what type of stakeholder you are.

SSL provides a mathematically-based secure connection (or channel) between two computers and then encrypts all subsequent communications. One portion of the protocol allows two computers to stay connected via use of a 'heartbeat' mechanism even when no activity exists (with one computer effectively saying "I'm here. Are you there?" and the other computer responding accordingly). This allows a connection to persist even in the absence of active communications. The vulnerability was disclosed publicly on Monday by a group of U.S. and Finnish researchers who found that the heartbeat mechanism could be forced to erroneously return a large block of data. The major concerns is that the block of data could contain sensitive information.

The Heartbleed vulnerability involves only one version of the SSL protocol known as OpenSSL, but OpenSSL happens to be among the most widely used versions of SSL. While the extent of the exposure is a concern, there are two other issues revealed by this disclosure that also raise concerns from a mitigation perspective. First, the vulnerability has potentially existed for over two years. This means any communications secured by OpenSSL deployments over the past two years *could have* been exposed to hackers. It *does not* mean all of those communications actually were compromised. The second troublesome point is that some theoretical exploits of the vulnerability leave no forensic evidence that an attacker was present on an affected server. This means that traditional techniques for investigating and determining whether there have been any security breaches may not work.

Some takeaways (which will dispel some rumors along the way):

- You do NOT need to stop using the Internet—even temporarily (despite news reports to the contrary; no, the sky is not falling and the Internet is not broken).
- The vulnerability only exists in one SSL implementation—the open source version known as OpenSSL. Other implementations (including custom written versions) are not known to contain this vulnerability.
- While the extent of the problem has not yet been quantified because it (currently) cannot be measured, not all communications have necessarily been compromised. It would take a very specific set of circumstances to reveal sensitive data. This is an important thing to know as you read some of the other more inflammatory reports that claim that all communications have been compromised.
- Now that the vulnerability has been disclosed, researchers and hackers are engaged in a race to fix (in the former case) or exploit (in the latter case) the problem.

You should also consider doing the following if you are a corporate/enterprise stakeholder that has implemented SSL or uses a service provide that has implemented SSL:

- Determine if you have deployed OpenSSL in any of your products or services, or if any of your service providers have done so. If so, consider an upgrade asap.
- Analyze web and cloud services that you use for use of OpenSSL. Contact any entities that may be vulnerable. Work with your technical and legal teams to respond accordingly.
- Consider changing any sensitive information that may be critical on a going forward basis (e.g., passwords, public/private key pairs, security questions and answers, etc.)

ADDITIONAL INFORMATION

US-CERT **alert**

The Vulnerability Notes Database sponsored by US-CERT/DHS and the Software Engineering Institute at Carnegie Mellon University **vulnerability note**

Several sources of technical information are becoming available, including: **heartbleed.com**, **F5 Networks** and **Symantec**

OpenSSL organization **advisory**

A purported **test for vulnerable sites**

Key Contacts

Matthew D. Brown San Francisco	brownmd@cooley.com +1 415 693 2188
Adam Ruttenberg Washington, DC	aruttenberg@cooley.com +1 202 842 7804
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090