the Availability Digest

www.availabilitydigest.com
@availabilitydig

Heartbleed – The Worst Vulnerability Ever

April 2014

Heartbleed is a flaw in the OpenSSL (Open Secure Sockets Layer) cryptographic software library. OpenSSL provides the security functions for the Internet Transport Layer Security protocol (TLS). SSL/TLS provides communication security over the internet for applications such as web email, instant messaging (IM), and some virtual private networks (VPNs).

Heartbleed allows attackers to read memory data from client and server devices to obtain private keys, passwords, and user names. It can then use this information to decrypt communications to and from these devices and to attack user accounts on other web sites.

Heartbleed leaves no traces of its activity. It was introduced in a released version of OpenSSL in March, 2012, and was not discovered until April, 2014. For over two years, it has been available for malicious use to compromise web sites and mobile devices. It is estimated that 17% of all secure web sites use the flawed version of OpenSSL. The rush is on to upgrade these systems with the corrected version of the software.

What is Heartbleed?

OpenSSL is relied upon by many organizations to secure their websites and the communications with them. Users are typically notified that a website is protected via an HTTPS (Hyper Text Transfer Protocol Secure) lock icon.

Heartbleed allows hackers to bypass the OpenSSL protection. Attackers can read portions of memory of a protected device. This memory may include the private keys used by OpenSSL for public/private key encryption as well as usernames and passwords that may be stored on the affected device.

Knowing a device's private key, attackers can monitor encrypted communications between the device and other systems. An attacker can also use the key to impersonate the device.

Knowing usernames and passwords, hackers can access email, IMs, and business-critical documents. User accounts on other systems can be accessed to steal personal data or money.

With all of this malicious capability, Heartbleed leaves no traces. There is no log activity that records its intrusion. It is virtually impossible to detect. This is one of the reasons that it remained undetected from the release of the flawed version of OpenSSL on March 14, 2012, until the vulnerability's discovery on April 1, 2014, a period exceeding two years.

Affected versions of OpenSSL are versions 1.0.1 to 1.0.1f. Versions 1.0.0 and earlier and versions 1.0.1g and later do not carry the flaw.

According to *Forbes* cybersecurity specialist, Joseph Steinberg, “Some might argue that [Heartbleed] is the worst vulnerability found (at least in terms of its potential impact) since commercial traffic began to flow on the Internet.”

How difficult is it to crack a system’s security with Heartbleed? A major cloud provider, CloudFare, stated publicly that it was extremely difficult and probably not a real threat. To prove its point, it ran a contest to see if anyone could steal its keys. Almost 3,000 hackers took the challenge, and six managed to get the keys over a weekend. CloudFare has recanted its statement and is changing all of its keys and security certificates.

The OpenSSL project was started in 1998. As of 2014, two-thirds of all secure web servers use it. The entire OpenSSL development group comprises ten volunteers and one full-time employee. The project has an annual budget of less than USD $1 million, though the project is now sponsored by the U.S. Department of Homeland Security and the U.S. Department of Defense.

How Does Heartbleed Do It?

The OpenSSL flaw that opened the Heartbleed vulnerability was a missing bounds check in handling TLS heartbeats. Heartbeats were added to OpenSSL in version 1.0.1, which was released on March 14, 2012. The intent of the heartbeat was to test and keep alive secure communication links without the need to renegotiate the connection.

Either side can send a heartbeat to the other side, and the initiator expects a copy of its heartbeat in response. The heartbeat is an arbitrary text string, up to 64K bytes in length, and a 16-bit integer indicating the length of the text string. For instance, the heartbeat message might be “bird, 4.”

Unfortunately, the flawed heartbeat logic in OpenSSL did not check the text message against the indicated length (the missing bounds check). If the initiator of the heartbeat sent a heartbeat comprising “bird, 64K,” it would receive the text “bird” followed by 64K bytes (less four bytes) of the following contents of memory.

That chunk of memory could then be mined for information nuggets. It was typically dynamically allocated memory used by OpenSSL and contained data such as private keys, user names, and passwords. Since the memory block returned as a heartbeat response was taken from dynamically allocated memory that had been returned to the memory pool, each heartbeat typically received a different block of old memory that contained different information.

To take advantage of this flaw, all an attacker would have to do is to send the malformed heartbeats. The only question was how many it would take in order to obtain useful information. A measure of this can be estimated from the CloudFare experiment. It took 44 million hacking attempts from 3,000 hacker IP addresses to yield six hits – a little more than one success per 10 million attempts. Tough, but certainly doable.

How was Heartbleed Found?

Coincidentally, the Heartbleed flaw was found almost simultaneously by two organizations – Google and Codenomican. Google’s research team found it on April 1, 2014. Codenomican’s team found it on April 4th.

Codenomican is a Finnish cybersecurity company founded in 2001 by Finnish security experts. With offices in a half-dozen countries, Codenomican focuses on testing software for bugs and writing patches to correct them. Their customers include Verizon, Microsoft, and Adobe.

Once Codenomican discovered the bug, it tested the bug by attacking itself, which it did successfully. As did Google, Codenomican kept the vulnerability a secret until it had created a fix for the flaw. When the patch was available, it announced Heartbleed on April 7th.

Codenomican recognized the seriousness of the Heartbleed vulnerability, but it was concerned that no one would notice the impact of the bug based just on its announcement. To bring attention to Heartbleed, it named it (the OpenSSL heartbeat was bleeding information), created a logo, and started a website (www.heartbleed.com) that was available on the announcement day. Codenomican succeeded in drawing attention. The Heartbleed website had 1.4 million accesses in the first two days.

Heartbleed and Mobile Devices

Google has confirmed that its Android version 4.1.1 has the Heartbleed vulnerability. This version was released in 2012 to the smartphone and tablet manufactures, and it is used on an estimated 50 million Android devices worldwide.

As of this writing, Google has not issued a patch to correct the vulnerability. Even when it does, there is no easy way to correct the flaw in the affected Android devices. Updating the Android operating system is up to the handset makers and the wireless carriers, and their update cycles tend to be very long.

Verizon has stated that iPhones are not affected. Apple does not use the vulnerable version of OpenSSL in its iPhones or iPads.

Microsoft has said that neither Windows phones nor the Windows operating system is affected.

Heartbleed and the NSA

Shortly after the announcement of Heartbleed, Bloomberg News published a report citing two anonymous sources alleging that the U.S. National Security Agency (NSA) was aware of the Heartbleed bug for the two years of its existence. NSA failed to report the flaw and exploited it instead to gather critical intelligence.

NSA flatly denied the report. According to an NSA spokesperson: “NSA was not aware of the recently identified vulnerability of OpenSSL, the so-called Heartbleed vulnerability, until it was made public in a private-sector cybersecurity report. Reports that say otherwise are wrong.”

The Director of National Intelligence said that vulnerabilities are disclosed as soon as discovered unless there is a clear national security or law enforcement need to do otherwise.

Protecting Against Heartbleed

Now that a corrected version of OpenSSL has been released, operating system vendors, product suppliers, and service providers must notify their users if their software systems were exposed to the vulnerability. If so, they must upgrade their systems and release the patched versions immediately.

Products using the flawed versions of OpenSSL do not have the bug if OpenSSL was compiled with the NO_HEARTBEATS option. Unfortunately, heartbeats are the default.

Affected users must perform the following tasks once they have upgraded their systems to a corrected version of OpenSSL:

- All applications must be restarted, since otherwise the software will continue to use its in-memory copy of the OpenSSL code.

- All compromised private key-public key pairs must be regenerated.

- All certificates linked to compromised key pairs must be revoked and replaced.

- All passwords to possibly compromised servers must be changed.

See Wikipedia and the Heartbleed website for lists of affected web sites and operating systems.

Summary

The Heartbleed vulnerability has been aggravated by several factors:

- It has been around for a long time (two years).
- It is relatively easy to exploit.
- It leaves no trace.

The good news is that it appears that hackers have not discovered the Heartbleed vulnerability in its two years of existence, just as the security specialists have not. There have been no major reports of stolen data due to Heartbleed, though the Canada Revenue Agency closed down its website on April 8th when it reported that 900 Social Insurance Numbers had been stolen in a six-hour period.

This good news may not be true of government agencies, which are more focused on finding security vulnerabilities for intelligence gathering. These agencies often employ large groups of security specialists for just this purpose. NSA is reported to have about 1,000 security specialists focused on this task.

Heartbleed begs the question as to whether open-source software is more secure than proprietary software. This is often an assumption, though it may be naïve. Open-source projects are often manned by small teams of developers – sometimes even a solo developer. They do not have the time and resources that most quality-assurance departments have for ensuring dependable, secure software.

Acknowledgements

Material for this article was taken from the following sources:

Change Your Passwords: A Massive Bug Has Put Your Details at Risk, *Time*; April 9, 2014.
Panic on web as Heartbleed bug leaves millions of users vulnerable, *The Times of India*; April 9, 2014.
Behind the Scenes: The Crazy 72 Hours Leading Up to the Heartbleed Discovery, *Vocative*; April 10, 2014.
NSA Said to Exploit Heartbleed Bug for Intelligence for Years, *Time*; April 11, 2014.
NSA Denies Knowing About Heartbleed Bug, *Time*; April 11, 2014.
Millions of Android Devices Vulnerable to Heartbleed Bug, *Bloomberg News*; April 12, 2014.
Heartbleed hackers steal encryption keys in threat test, *itpro*; April 15, 2014.
Heartbleed: 50m Android phones may be affected, report shows, *Independent*; April 21, 2014.
Heartbleed.com
Heartbleed, *Wikipedia*
OpenSSL, *Wikipedia*.