the Availability Digest

www.availabilitydigest.com
@availabilitydig

Heartbleed Attacks Androids

May 2014

Heartbleed is a notorious Internet vulnerability that was introduced in 2012, but it only came to light recently. It allows a malicious attacker to steal data from a device in an undetectable way as its browser is used.

Heartbleed has had tremendous media exposure, and most people now know about it. If you are one of those and have taken the precaution of upgrading your browser and changing all your passwords, you may think that you are now safe. However, if you are an Android user, think again. There is a long way to go to make Android devices safe from Heartbleed. Though you may have received Google's patch to correct the vulnerability in your Android operating system, you may be running several apps that open up your device to a Heartbleed attack.

What Is Heartbleed?

We described the Heartbleed vulnerability in our last issue of the Availability Digest.[1] To recap, Heartbleed is a flaw in the open-source OpenSSL (Open Secure Sockets Layer) cryptographic software library used to provide communication security over the internet via encryption.

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. With all of its malicious actions, Heartbleed leaves no traces. There is no log activity that records its intrusion. It is virtually impossible to detect.

The OpenSSL flaw that opened the Heartbleed vulnerability was a missing bounds check in handling 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.

[1] Heartbleed – The Worst Vulnerability Ever, *Availability Digest*; April 2014.
http://www.availabilitydigest.com/public_articles/0904/heartbleed.pdf

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. Each block of memory could then be mined for information nuggets. Because the blocks were typically dynamically allocated memory used by OpenSSL, blocks often contained data such as private keys, user names, and passwords.

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.

Android and Heartbleed

Android versions 4.1.0 and 4.1.1 (released in 2012) contain the Heartbleed vulnerability. About 20% of all Android phones use these versions of the operating system (mostly version 4.1.1). Consequently, about 50 million Android phones worldwide may be vulnerable. People using these versions should avoid sensitive transactions because their data may be compromised. Opening a malicious website as a result of a phishing email may allow a hacker to take advantage of the Heartbleed bug to steal data from the phone.

Google has released a patch to the Android operating system to correct the vulnerability. However, it may take some time for this patch to reach phones in the field as updates must come from the smartphone manufacturers and wireless carriers. They typically make updates only every few months, so protecting the flawed Android phones may take some time.

Android Apps and Heartbleed

But this not the end of the story. Just because the Android operating system has been patched does not mean that a phone's vulnerability has been corrected. This is because the vulnerability also exists in a myriad of Android apps – even those available through Google's Google Play app store.

Android apps frequently use native libraries, which either directly or indirectly leverage vulnerable OpenSSL libraries. Though developers have corrected many of their apps, many more continue to carry the flaw. The corrections to some may be long in coming, if ever. For instance, many apps use embedded URLs over which the developer has no control. Other apps are no longer maintained.

Security firm FireEye[2] scanned 54,000 Google Play apps, each with over 100,000 downloads, and determined that 220 million of these downloads contained the Heartbleed vulnerability. No patches are yet available for these apps. Many of these were business apps, making the risk of sensitive data loss even greater. It is quite likely that many 4.1.0 and 4.1.1 Android users who now feel protected are still open to a Heartbleed attack.

Detecting Heartbleed Vulnerability

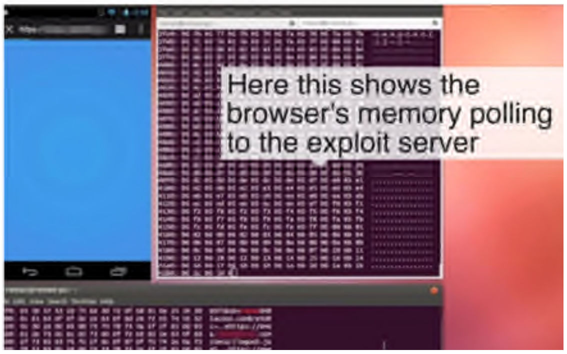
FireEye found seventeen apps in Google Play that purport to detect whether an Android phone is infected by Heartbleed. Some only scanned the operating system, not the apps. Some were fakes and did no scanning – they were only adware. FireEye found only two apps that were effective. Unfortunately, they did not identify these two apps in their publication referenced above.

Lacoon Mobile Security is another security firm focused on Heartbleed. They have produced a YouTube video showing the ease with which a vulnerable Android phone can be attacked.[3] The video shows pages of data being pulled from an Android phone's memory, exposing passwords and other valuable data, as

[2] If an Android Has a Heart, Does It Bleed?, *FireEye*; April 22, 2014.
http://www.fireeye.com/blog/technical/2014/04/if-an-android-has-a-heart-does-it-bleed.html

[3] Bleeding in the Browser, *Lacoon Mobile Security.*
https://www.youtube.com/watch?v=bzKrtm7rFlc

the phone's browser accesses Salesforce.com and Facebook.com. Neither of these web sites are vulnerable to Heartbleed. Rather, the bleeding is between the phone and a malicious server.


Here this shows the browser's memory polling to the exploit server

Lacoon Mobile Security

Lacoon also has posted another video to YouTube showing the detection and protection of an Android phone against a Heartbleed exploitation using their mitigation product MobileFortress.[4] MobileFortress includes a gateway to inhibit heartbeats until the phone is free of vulnerabilities. With no heartbeats, no data will be stolen. The only impact is that connections will not be retained and will have to be reestablished.

Summary

Heartbleed has been one of the worst vulnerabilities ever to hit the Internet because it easily steals data from servers and client devices. It is so transparent that it took two years to expose. Most servers have by now been corrected. However, millions of Android phones are still vulnerable to data loss from malicious servers because the Heartbleed flaw is contained in thousands of Android apps. It may take a long time to correct all of these apps and to render the phones invulnerable to Heartbleed. Some vulnerable apps may never be detected or corrected.

Apple states that it does not use the vulnerable version of OpenSSL in its iPhones or iPads. Microsoft says that its Windows Phones and its Windows operating system are not affected. This includes Windows XP, which Microsoft patched even though it had ceased to provide updates for Windows XP. According to a Microsoft statement:

> "Even though Windows XP is no longer supported by Microsoft and is past the time we normally provide security updates, we've decided to provide an update for all versions of Windows XP, today. We made this exception based on the proximity to the end of support for Windows XP."

Acknowledgements

In addition to the references cited above, information for this article was taken from the following sources:

Heartbleed Bug Puts Millions of Android Devices at Risk, *Huffington Post*; April 15, 2014.
Android Heartbleed Alert: 150 Million Apps Still Vulnerable, *Dark Reading*; undated.
Why Heartbleed could be much worse for Android users, *BGR*; April 16, 2014.
Millions of Android App Downloads Are Vulnerable to Heartbleed Bug; *Infosecurity Magazine*; April 23, 2014.
What a Heartbleed Attack on an Android Phone Looks Like, *Bloomberg*' April 29, 2014.
Millions of Android apps still affected by Heartbleed, *CSO*; April 29, 2014.
Microsoft fixes flaw in Internet Explorer on XP despite end of security patches, *The Guardian*; May 2, 2014.
Heartbleed: 50m Android phones may be affected, report shows, *Independent*; May 16, 2014.

[4] How Mobile Users Can Protect Themselves From Heartbleed, *Lacoon Mobile Security.* http://www.youtube.com/watch?v=8vqSaf0hGtc&src_vid=bzKrtm7rFlc&feature=iv&annotation_id=annotation_3301605335