Is Cloudbleed Inevitable After Heartbleed?

By Taiye Lambo and Jordan Flynn

September 2014

In the technology world, vulnerabilities and bugs are commonplace. Whether an avid hobbyist or a professional working for an organization in a technical capacity, those familiar with the technology and information security space understand that there is no avoiding the inevitable discovery of vulnerabilities and bugs that must ultimately be addressed.

While some of these fixes require nothing more than a simple patch job, others necessitate significant changes in policy and process within the workplace and the cautious or discontinued use of applications on mobile devices and Internet based services. With the rise in cybersecurity attacks and the continued growth of individuals storing their sensitive information online, vulnerabilities in cyberspace represent one of the most significant concerns not just for hobbyists and professionals, but also for society as a whole.

The discovery of the Heartbleed bug in April 2014 made the issue of vulnerabilities and bugs in cyberspace more evident. Fundamentally, the vulnerability allows for anyone on the Internet to read and view the personal and sensitive information of others through system memory, information meant to be protected by the SSL/TLS encryption that is used to secure the vast majority of the Internet. Compounding this issue is that Heartbleed also provides the proverbial "key to the kingdom" by making the confidential keys used to properly identify service providers, and encrypt the names and passwords of users as well as actual content itself available to the criminal, allowing them to easily spy on communications and impersonate both users and services therefore stealing sensitive data directly from them.

However, what is most alarming about Heartbleed is how long it took to discover the vulnerability and how it has affected the average consumer. Rather than being a bug or vulnerability restricted to a business network or environment, Heartbleed affects individuals in their everyday life as they use the Internet to complete personal financial transactions and manage their sensitive and personally identifiable information on a near daily basis. Prior to the discovery of Heartbleed, it is estimated sensitive consumer data was vulnerable in excess of five months.

While the Heartbleed bug has taught us many hard lessons, there remains an estimated 300,000 websites that have not yet patched the vulnerability, showing a surprising lack of initiative in not only detecting, but responding to these types of attacks. One of the most important responses to this type of attack is using the experience as a tool to predict, prevent and prepare for future events that may likely occur as a natural extension of said event. As virtually everyone with a phone, laptop or Internet connection utilizes cloud services in some capacity, the question must be asked whether a "Cloudbleed" is inevitable following the Heartbleed breach.

With all three major cloud service models relying on significant vectors that can be attacked and exploited, consumers should be prepared for a Cloudbleed event in the near future.

Infrastructure as a Service (IaaS) cloud services act as the foundation of all cloud offerings, and sits in a precarious position. Because cloud infrastructure resources (processing power, storage, etc.) can be actively provisioned and scaled almost infinitely to support a large number of businesses and personal needs, it is a natural target for criminals seeking to disrupt entire services and supply chains to gain access to sensitive information. The main concern is in the use of cybersecurity attacks on HVAC systems used to support the servers and equipment needed to provide essential cloud services.

HVAC security is not commonly addressed from a cybersecurity perspective by businesses and service providers, mixed with a lack of anti-virus and anti-malware available for such systems, the opportunity exists for criminals to discover common weaknesses within these support systems and exploit them to attack data centers delivering Infrastructure as a Service, forcing hard resets of systems supporting entire services to gain entry to sensitive information on a massive scale. The Target breach disclosed in December 2013, one of the largest data breaches in history at 110 million customers affected, occurred through a 3rd party HVAC vendor. With the cloud being used to support massive arrays of networks and ecosystems, the effects of a Cloudbleed event within the IaaS service model could increase the scale of such attacks to almost incomprehensible levels, and represents a significant threat to be aware of and prepare for in the near future.

Platform as a Service (PaaS) cloud services, which are used to develop and manage applications and automate configurations, are also in danger of experiencing a Cloudbleed event. With the emergence of virtualization technologies and their increasing use with cloud services, the PaaS deployment model may be exploited by criminals targeting virtual machines and, especially, the hypervisor level. While virtual machines present a number of threats and ways for criminals to find common vulnerabilities, from VM Sprawl to ineffective network controls and active migration concerns, it's the hypervisor level that represents the most substantial concern to the PaaS service model because once an attacker gains access to the hypervisor, its game over. The hypervisor is the Achilles heel of PaaS because once accessed, the entire cloud and all of its virtual machines are at tremendous risk. With the jury still out on how to best harden the hypervisor and no current best practices available for checking hypervisor security violations, a potential Cloudbleed event at the PaaS level remains a high risk.

Finally, Software as a Service (SaaS) cloud services have been shown to be particularly vulnerable, with the recent Google Gmail, Apple iCloud, CodeSpaces and eBay hacks proving that attacks on user credentials are often successful enough to do significant damage, acquire sensitive information or, as in the case of CodeSpaces, destroy a cloud service entirely, the nightmare scenario for the cloud. Unfortunately, many SaaS providers lack the basic controls and awareness that would otherwise prevent such attacks. For example, Apple iCloud did not implement a lock out procedure for users after a set amount of unsuccessful password attempts was met, nor did it extend its recent multi-factor

authentication feature across all of its iCloud services, allowing brute force attacks to be carried out against passwords and access to sensitive information easily obtained.

CodeSpaces, meanwhile, did not implement simple role-based security management practices nor did they require multi-factor authentication, all factors that played a substantial role in this cloud service provider's downfall. Many of these controls are simple controls to implement yet remain one of the weakest links for many cloud service providers, particularly SaaS providers.

CloudeAssurance's independent cloud security benchmark entitled "Top 10 Cloud Service Providers" corroborates this truth with its ongoing research into the Top 10 Cloud control gaps, which identifies lack of user password management features such as account lockout to prevent brute force attacks against passwords as well as a lack of multi-factor authentication implementation as top gaps in the cloud space.

With the recent media coverage of cloud related breaches we must prepare for a potential Cloudbleed event against all cloud service models, and both providers and consumers alike must become more educated and aware of the steps they can take to prevent a future Cloudbleed event or minimize the impact of such event.

About the Authors:

Taiye Lambo is a seasoned entrepreneur with Global Information Security and Governance, Risk Management and Compliance expertise with a focus on Cloud Computing. He is the inventor of the innovative AlertApp! and Founder of USA based CloudeAssurance, Inc., eFortresses, Inc., the Holistic Information Security Practitioner Institute (HISPI) and the UK Chapter of the Honeynet Project.

He can be contacted via E-mail (tlambo@eFortresses.com), LinkedIn (http://www.linkedin.com/in/taiyelambo) or Website (www.CloudeAssurance.com).

Jordan Flynn is the Lead Cloud Security Analyst and Researcher for the CloudeAssurance platform, with a focus on the application of cloud computing best practices, global standards, and enterprise governance, risk and compliance, in particular cloud security framework management and risk assessment methodology. He heads the CloudeAssurance independent cloud security benchmark study entitled "Top 10 Cloud Service Providers", which names the Top 10 Cloud Service Providers each quarter. He also operates as an information security consultant with an emphasis on the NIST Cybersecurity Framework, ISO 27001, and PCI-DSS 3.0.

He can be contacted via E-mail (JFlynn@eFortresses.com), LinkedIn (https://www.linkedin.com/pub/jordan-flynn-ccsk-hisp/2b/1b3/9b8) or Website (www.CloudeAssurance.com).