The Heartbleed Bug: How To Protect Your Business with Symantec

Who should read this paper

Information security professionals who want to understand how to protect their systems from Heartbleed vulnerability.
Introduction

On April 7, 2014, a team of security researchers announced the discovery of a critical vulnerability found in certain versions of the widely used OpenSSL cryptographic software library. This bug would become known as “Heartbleed,” and its arrival exposed a serious vulnerability in OpenSSL, allowing attackers to access and read the memory of web servers running vulnerable versions of the library.

These systems, and the information they house, are normally protected by the SSL/TLS encryption used to secure data in transit across the Internet, which provides privacy for communications applications on the Web such as e-commerce, banking, email, and instant messaging. However, Heartbleed has been known to compromise these systems and the private keys used to identify service providers and encrypt user authentication and the data they need secured. The result? Attackers can intercept communications data, steal information and passwords, and even impersonate those users’ online identities and illegally use their services.

OpenSSL

OpenSSL is an open-source cryptographic library often used with applications and web servers like Apache and Nginx, and in broader contexts with a variety of other operating systems, toolkits, software, and applications. Its usage is ubiquitous across the globe—Apache, the world’s most widely used web server when combined with Nginx, represents close to 54% of all web servers worldwide.

SSL sends a ping, or “heartbeat,” to the web server to keep encrypted sessions active. Heartbleed makes this process vulnerable to attack because an infiltrator can exploit this heartbeat by sending a malicious request to an affected server running a vulnerable version of OpenSSL. In short, the affected server will send back up to 64kb of data from its memory in order to match the request. Leaked information could include usernames, passwords, and private keys.

History

The detection of the bug itself happened in late March 2014, when Neel Mehta of Google Security discovered the Heartbleed vulnerability. That same morning, Google issued a patch on its servers and informed a few select companies. On April 1, 2014, the OpenSSL team was...

1 NetCraft March Web Survey, March 2014
The Heartbleed Bug: How To Protect Your Business with Symantec

notified. Soon after, Codenomicon, a Finnish cybersecurity company, also independently discovered the bug. The company is credited for naming the bug, creating the recognizable bleeding heart logo, and launching heartbleed.com as an information resource.

Recent Events Surrounding Heartbleed

Shortly after Heartbleed was revealed to the world, the Canada Revenue Agency fell victim to a data breach that leaked the Social Insurance Numbers of approximately 900 Canadian citizens. After learning of the bug, the agency immediately shut down its website to keep even more sensitive personal information from becoming comprised or stolen.

Soon after, the Royal Canadian Mounted Police reported the arrest of 19-year-old Stephen Arthuro Solis-Reyes at his London, Ontario home. During the raid, government agents seized computer equipment as evidence.

In addition, Mumsnet, a popular parenting advice website, has reported its user-data as stolen by hackers using the Heartbleed bug. Mumsnet founder Justine Roberts said in a statement that a recommended fix was applied immediately after the bug was discovered. However, she added that there was no way of knowing how many users had already been affected by the security breach.

As reports of further damage come in, it is clear that the effects of Heartbleed will greatly impact software companies and organizations that depend on Internet security to manage websites and build custom applications. In addition, some certificate authorities could continue to feel potentially debilitating effects by way of:

• Mass revocations
• CRL spikes
• Performance degradation
• CA costs increase

Symantec Protects Your Business—Today and Into the Future

Despite the widespread harm caused by Heartbleed, Symantec’s blend of industry-leading security solutions and Certificate Authority infrastructure products can not only heal the damage inflicted by the bug, but can also prepare companies to weather further, even more sophisticated attacks in the future.

Catastrophic attacks and breaches come in many ways, including predatory opportunists, international crime syndicates, sophisticated hackers, and even simple human error. One missed problem in the coding or an overlooked hole in the system can be disastrous to a company’s security story and cause irreparable harm. Organizations need a partner that not only understands how to protect infrastructures from the likes of bugs such as Heartbleed, but also from the myriad other ways in which a company's systems and information can be compromised, sabotaged, or stolen.

Symantec is poised to help protect organizations by helping them discover the vulnerabilities, remediate the damage through effective patching and repair, then helping to further protect critical data and resources from future incursion.

---

5- http://www.wired.com/2014/04/cost-of-heartbleed/
1) Discover

In order to protect an organization’s systems and infrastructure, a plan must be in place to discover the problems before they become disastrous. Symantec has the solutions to scour the entire infrastructure and discover problem areas with Vulnerability Assessments on SSL certificates that use industry-leading services and solutions.

**Symantec Control Compliance Suite (CCS)** is a modular vulnerability detection solution, made up of different components that are fully interoperable and available separately or as part of a broader suite.

**CCS Standards Manager** performs a network and asset discovery scan, allowing you to:

- Detect authorized vs. unauthorized hardware
- Conduct a software inventory to determine if OpenSSL is indeed installed
- Perform an evaluation to detect if an “at-risk installation” of OpenSSL exists on the asset, then scan for vulnerabilities

**CCS Vulnerability Manager** performs end-to-end vulnerability assessment of Web applications, databases, servers, and network devices, allowing you to:

- Deliver a single view of security threats across your IT infrastructure
- Run authenticated Heartbleed checks for supported Linux platforms as well as platform-independent remote checks
- Test defenses and assess the impact of Heartbleed in your environments

**CCS Vendor Risk Manager** conveys the impact of IT risk in business-relevant terms, allowing you to:

- Detect at-risk networks and assets and make recommendations on how to best prioritize remediation efforts
- Identify the most critical third party partners and programmatically reach out to determine which of these partners are vulnerable to Heartbleed

**Symantec Certificate Intelligence Center (CIC)** is an efficient certificate management tool that discovers, tracks, and automates the SSL Certificate lifecycle with the tools organizations need to provide critical discovery and business continuity.

**CIC** provides built-in SSL certificate automation capabilities that:

- Eliminates human error in certificate management, and installation overhead
- Streamlines the process of renewing, transferring, and installing digital certificates

**CIC** delivers certificate discovery and business continuity that empowers businesses with:

- Clear visibility of every SSL certificate deployed across the network
- Rich reporting functionality with notification capabilities that help administrators make well-informed decisions quickly

2) Remediate

Once system vulnerabilities are discovered, Symantec has the solutions in place today to remediate the issues and take whatever steps are necessary to repair, including:

- Identify domains that are hosted on affected servers
- Patching or recompiling
Replacing affected SSL Certificates  
Testing  
Revoking the certificates that were installed on affected servers  
Installing validation and ID protection in order to mitigate any possibility of exploitation of compromised data

The first step is to check domains by using Symantec’s free SSL toolbox. There are no limits, sign-ups, or ads, and the tool can be used throughout the entire remedy process. Then, patch or recompile. If you discover your domain is vulnerable, you have three main options:

- Roll back before OpenSSL 1.0.1
- Update to version 1.0.1g
- Recompile OpenSSL without the Heartbeat extension

Next, replace any affected certificates. It’s always smart to use a new private key before generating a new CSR. Many think that simply generating a new CSR will resolve the problem—however, a Heartbleed attack and can exposed your private key. Symantec recommends that if you haven’t moved to SHA-2, you should right away. Microsoft has announced that it will be blocking the use of SHA-1 after January 1, 2017.

Finally, using the same tool as in the first step, check to ensure your certificate is correctly chained. Then you can safely revoke any and all replaced certificates.

Heartbleed is a wake-up call for companies of all sizes to implement two-factor authentication (2FA), and Symantec Validation and ID Protection Service (VIP) provides that much-needed second factor so even if a user’s password is compromised, their account remains protected.

Having VIP protection means that the infiltrator must do more than simply get through your firewall with your stolen password—they would also be required to present a second credential for authentication. VIP is a cloud-based service that provides strong authentication with a variety of authentication options, and a choice of credentials. Most popular is the easy-to-use mobile credential, which generates the 6-digit security code on the mobile device. These codes expire in 30 seconds and can only be used once, making them very difficult to steal. The new Push verification for Mobile Access provides the option of either confirming or denying an authentication attempt with the push of a button (no need to even enter the 6-digit code). Whether or not you use the one-time password or the push verification, if the second factor is not presented, the attacker is locked out.

**Symantec IT Management Suite** powered by Altiris technology makes it possible to manage the entire lifecycle of desktops, laptops, servers, and virtual machines. One of the key capabilities includes the efficient delivery of applications and patches to vulnerabilities such as Heartbleed. IT Management Suite allows you to:

- Determine which computers are running versions of OpenSSL that are vulnerable to Heartbleed
- Distribute software updates for OpenSSL throughout your network to eliminate the Heartbleed vulnerability
3) Protect

To this day, a surprising number of organizations rely solely on passwords for network authentication and access to applications—and Heartbleed gives attackers what they need to steal all of your users’ passwords and ultimately their accounts and identities. A powerful tool that protects users from threat is Symantec Endpoint Protection. Symantec Endpoint Protection 12.1 detects and blocks attempts to exploit the Heartbleed vulnerability on endpoints.

**Symantec Endpoint Protection** includes a layered approach to defense, and combined with granular controls, enables businesses to stay ahead of advanced threats. All of the following technologies work with Symantec Endpoint Protection:

- **Network Protection:** Most known threats can be blocked as they travel over the network and try to take up residence on a system. This primary defense protects against drive-by downloads, social engineering, fake-antivirus, individual system vulnerabilities, rootkits, botnets, and more. Needless to say, stopping malware *before* it reaches your system is preferred to identifying a vulnerability that has already been exploited.

- **File Protection:** Traditional signature-based antivirus that looks for and eradicates malware that has already taken up residence on a system is ubiquitous. Unfortunately, many companies leave themselves exposed through the belief that antivirus alone is going to keep their systems protected.

- **Reputation Protection:** Sophisticated threats require leveraging the collective wisdom of over 200 million systems to identify new and mutating malware. With Symantec Insight, companies have access to currently the largest global intelligence network in the industry to allow them to filter every file on the Internet, based on reputation.

- **Behavior Protection:** Aggressively monitoring file processes as they execute and identifying malicious behavior can catch targeted and unknown threats. Symantec SONAR uses artificial intelligence, behavior signatures, and policy lockdown to monitor nearly 1400 file behaviors as they execute in real time. When combined with Insight, this technology is able to aggressively stop zero-day threats without spiking false-positives.

- **Repair and Remediation:** When malware does get through, Symantec Power Eraser can scrub hard-to-remove infections and get your system back online as quickly as possible.

For Heartbleed specifically, the IPS technology inside the Network Protection layer blocks the most common attack areas by stopping the threat before it takes residence on the endpoint.

**Conclusion**

Thinking ahead, preparing a proactive plan, and staying in front of the next big thing are all key to an organization’s overall security success. Symantec not only has a comprehensive suite of solutions to effectively discover and remediate vulnerabilities today—no matter their origin—but also has the thought leadership and world-class expertise to stay ahead of the next “Heartbleed.”

Visit [http://go.symantec.com/outbreak/](http://go.symantec.com/outbreak/) to learn how Symantec can help you today, and into the future.
About Symantec
Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data-intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company’s more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.