Venafi Labs Analysis

Hearts Continue to Bleed
Heartbleed One Year Later

Vast Majority of Global 2000 Organizations Remain Vulnerable to Cyberattacks

VENAFI

Executive Summary

Using the recently released Venafi TrustNet certificate reputation service, the Venafi Labs team re-evaluated SSL/TLS vulnerabilities in Q1 2015 and found that most Global 2000 organizations have failed to completely remediate Heartbleed—now a full year after the vulnerability was first publicly disclosed.

This leaves these organizations vulnerable to cyberattacks, future brand damage, and intellectual property loss. In one oft-cited incident, Community Health Systems was breached by the Chinese APT 18 group, who exploited incomplete Heartbleed remediation and unprotected keys to steal data on 4.5 million patients.[1]

When the Heartbleed vulnerability was disclosed in April 2014, many organizations scrambled to patch the bug, but failed to take all of the necessary steps to fully remediate. As of August 2014, 76% of the Global 2000 organizations with public-facing vulnerable systems were still vulnerable, failing to fully remediate based on specific guidance from Gartner and other industry experts.[2, 3]

3 out of 4 Global 2000 with public-facing systems vulnerable to Heartbleed are still open to breach.

Unfortunately little progress has been made to complete remediation and remove the threat. As of April 2015, 74% of the Global 2000 with public-facing vulnerable systems are still vulnerable. That's only a 2% improvement in 8 months, still leaving almost 3 in every 4 of these companies open to breach. Action remains needed and should be taken to find and replace affected private keys.

Ponemon Institute research that surveyed over 2,300 IT security professionals echoes this reality: 60% of participants agreed their organization needs to better respond to vulnerabilities involving keys and certificates like Heartbleed.[4]

Background: Heartbleed Vulnerability

Heartbleed is a vulnerability in OpenSSL 1.0.1 through 1.0.1f (inclusive). This vulnerability allows an attacker to extract data that includes SSL/TLS keys for X.509 digital certificates from the target without hacking the environment or being detected. From the start, it was clear that Heartbleed was not just another "patch-it" event. It struck at the core of what creates online trust: SSL keys and certificates. If SSL keys and certificates could be compromised, websites could be spoofed for phishing attacks and encrypted communications decrypted via man-in-the-middle (MITM) tactics resulting in customer data loss and intellectual property theft.

To fully remediate Heartbleed, SSL keys and certificates needed to be replaced.

Immediately after the Heartbleed vulnerability broke, experts from Bruce Schneier to Gartner's Erik Heidt made it clear that to fully contain and remediate Heartbleed, SSL keys and certificates needed to be replaced.[2, 3] In addition to applying the OpenSSL patch, organizations should generate new keys, issue new certificates, and revoke old certificates. If these actions were not taken, stolen keys could allow websites to be impersonated and traffic to be decrypted.

Although the Heartbleed vulnerability was disclosed to the public in April 2014, cybercriminals were aware of the vulnerability long before that. The Electronic Frontier Foundation confirmed Heartbleed related exploits occurred in November 2013,[5] while other analyses suggest possible exploits date back three years.[6] As a result, enterprises should assume adversaries have executed attacks using the exposed keys and certificates for some time.

The University of Maryland performed analysis in November 2014 to evaluate how well organizations had responded to Heartbleed. The researchers validated the Venafi July 2014 findings that 97% of Global 2000 publicly-facing servers were not remediated—leaving 76% of the Global 2000 with public-facing vulnerable systems still susceptible to Heartbleed exploits. The University of Maryland reported that, as of November, 87% of public-facing servers had not remediated according to Gartner guidance and were still vulnerable.[2, 7]

Precarious Situation for G2000 Organizations

Venafi Labs frequently analyzes the websites of Global 2000 organizations and the Alexa Top 1 Million to identify SSL/TLS vulnerabilities.[8, 9] We found that although many organizations believe they are no longer susceptible to Heartbleed, the data shows otherwise.

Even though many Global 2000 organizations have taken basic steps to remediate Heartbleed, most have not entirely remediated the vulnerability. Using Venafi TrustNet, Venafi Labs evaluated the 1,642 Global 2000 organizations with public-facing systems vulnerable to Heartbleed. As of April 2015, 74% of those scanned had not completed Heartbleed remediation across all public-facing servers. That's 1,223 of the world's largest and most valuable businesses still exposed to attacks. Only 419 Global 2000 organizations have completed Heartbleed remediation—up just 2% from 387 in August 2014.

Table 1. Global 2000 Heartbleed Remediation by Organizations
August 2014 vs. April 2015

	2014	2015
Vulnerable		
Incomplete Remediation	**76%**	**74%**
Remediation Complete	**24%**	**26%**

Cybercriminals have already used the keys and certificate that were captured via Heartbleed in well-known breaches like Community Health Systems where the group known as APT 18 stole data on 4.5 million patients.[1]

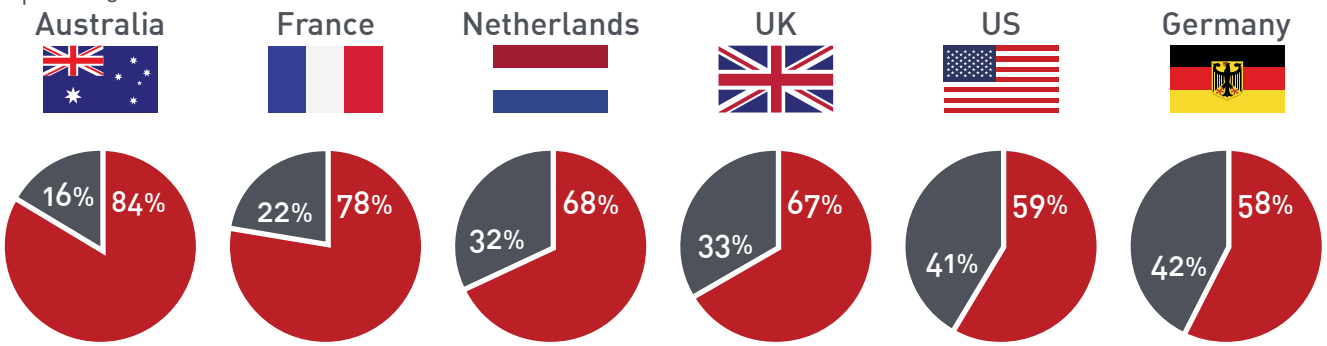
Incomplete Remediation: Why Hearts Still Bleed
Why have organizations still not completed full remediation? Organizations have either given up on properly replacing keys and certificates, most likely not grasping the full risk exposure this creates, or do not have the knowledge to understand how to complete remediation. As detailed by Gartner and industry experts such as Bruce Schneier, security teams must go beyond simply patching and also replace the private key, re-issue a new certificate, and revoke the old one.[2, 3]

Venafi has identified 580,000 hosts belonging to Global 2000 organizations that have not been completely remediated. These partially remediated hosts have been patched against Heartbleed. However, the organizations have either performed, as described by Gartner, "lazy" remediation, failing to replace the private key, or failed to revoke the old certificate.[2] Failure to replace the private key allows an attacker to decrypt any SSL traffic for the impacted host. Failure to revoke the old certificate enables the attacker to use the old certificate in phishing campaigns against the organization and its customers.

Remediation Complete
In 2015, 92,000 hosts, or 15% of Global 2000 organizations' hosts scanned, have fully remediated the Heartbleed vulnerability—a 16% improvement over 2014. This includes 65,000 certificates re-issued since 2014 with new private keys replaced because of impending certificate expirations. The standard practice for many using OpenSSL has been to simply

Table 2. Global 2000 Heartbleed Remediation by Country

April 2015



request new certificates with existing keys. However, Erik Heidt of Gartner chastised this approach as "'lazy' certificate rotation" and emphasized that new private keys must be generated. All keys and certificates "need to be retired and rotated."[2]

85% of Global 2000 external servers remain vulnerable to cyberattacks and compromise due to Heartbleed.

Enterprises must assume, just as they do with user IDs and passwords following an incident, that ALL keys and certificates are compromised, not just those that secured vulnerable Heartbleed systems. And attacks using keys and certificates are not theoretical. In Ponemon Institute research, 100% of the 2,300 IT security professionals surveyed acknowledged that they had responded to attacks using keys and certificates in the previous 24 months. However, properly rotating all keys and certificates is no easy task. According to the Ponemon Institute research, the average Global 2000 organization has almost 24,000 keys and certificates. To make this more challenging, 54% of organizations are unaware of where all of their keys and certificates are located.[3]

Also in the Ponemon Institute research, 60% of participants confirmed that their organization needs to better respond to vulnerabilities involving keys and certificates like Heartbleed. This Ponemon Institute research focused on 6 Global 2000 countries.[3] When Venafi Labs performed its Heartbleed analysis on these countries plus the Netherlands, the results revealed interesting trends. Table 2 shows the percentages of companies by country that have fully remediated Heartbleed versus those which are still vulnerable. Australia is by far the most behind at remediating Heartbleed while the United States and Germany lead remediation efforts—yet they both still have almost 60% of organizations without full remediation.

Kill chain analysis helps reveal that attackers look to expand their foothold by employing similar methods and targets as they used in their first intrusion. Since last year, there has been a significant increase in hijacked VPNs used to maintain access to victims' environments. Certificate-based, two-factor authentication is a common target. Further infiltration of networks means that SSL keys and certificates and SSH keys, even though not running vulnerable OpenSSL, should be assumed to be targets and compromised, and therefore replaced.

There are also hundreds of applications that operate behind the firewall that remain vulnerable to Heartbleed, including IBM, Juniper, Cisco, and many others. There is little information available on the state of remediation for these systems. However, remediation is likely no better than that for public-facing systems and may be worse. It is common for systems operating behind the firewall to have certificate expirations set for 3, 4, 5 years or much longer. Waiting for expirations to replace potentially compromised keys means Heartbleed vulnerable systems are not going away anytime soon.

Respond & Remediate Now

Remedation Steps
There are four basic steps to completing Heartbleed remediation:

- Know where all keys and certificates are located
- Generate new keys and certificates
- Replace new keys and certificates, revoke old ones
- Validate remediation to ensure new keys and certificates are in place and working

Learn More
You can see this guidance in practice in a case study for a Fortune 100 healthcare organization that used Venafi to fully remediate Heartbleed. Venafi also recently launched the Venafi TrustNet certificate reputation service to help organizations identify the misuse of certificates on the Internet and protect its subscribers' brand reputation. Find out more about TrustNet at Venafi.com/TrustNet.

You can also get details about an attack that used the Heartbleed vulnerability. Raxis, an independent penetration testing organization, reconstructed the APT 18 attack on Community Health Systems—a Fortune 500 healthcare company—to confirm its approach and effectiveness. To read about this APT 18 proof-of-concept attack, visit Venafi.com/APT18.

Complete Heartbleed Remediation Now
Are you one of the 3 out of 4 organizations that are still exposed to breach due to public-facing systems without full Heartbleed remediation? Or worse yet, are you also one of the 54% of organizations that are unaware of where all of their keys and certificates are located?[3]

Businesses need to complete Heartbleed remediation before they are breached. Venafi can help.

If you are, you're not alone, but it's time to do something about it before your business is breached. Venafi can help. With Venafi, you can identify your systems that still require Heartbleed remediation, find all of your keys and certificates, and automate reissuance and revocation processes.

Contact Venafi today to complete Heartbleed remediation and protect your business and brand.

Venafi.com/Contact

References

1. Bocek, Kevin. Venafi Blog. *Infographic: How an Attack by a Cyber-espionage Operator Bypassed Security Controls*. January 28, 2015.
2. Heidt, Erik T. Gartner Blog Network. *Heartbleed Exploit in OpenSSL – How Should You Respond?* April 9, 2014.
3. Schneier, Bruce. Schneier on Security Blog. *Heartbleed*. April 2, 2014.
4. Ponemon Institute. *2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point*. 2015.
5. Eckersley, Peter. Electronic Frontier Foundation. *Wild at Heart: Were Intelligence Agencies Using Heartbleed in November 2013?* April 10, 2014.
6. Riley, Michael A. Bloomberg Business. *NSA Said to Have Used Heartbleed Bug, Exposing Consumers*. April 12, 2014.
7. Zhang, Liang, et al. University of Maryland *Analysis of SSL Certificate Reissues and Revocations in the Wake of Heartbleed*. 2014.
8. Forbes Global 2000. *The World's Biggest Public Companies*.
9. Alexa. *Alexa Top Sites*.

About Venafi

Venafi is the market-leading cybersecurity company in Next Generation Trust Protection. Venafi delivered the first trust protection platform to manage, secure, and protect cryptographic keys and digital certificates that every business and government agency depends on for secure communications, commerce, computing, and mobility. Venafi customers are among the world's most demanding, security-conscious organizations.

Part number: 1-0040-0415