Venafi Labs Q3 Heartbleed Threat Research Analysis

Majority of Global 2000 Organizations Have Not Remediated Heartbleed, Remain Vulnerable to Cyber Attacks

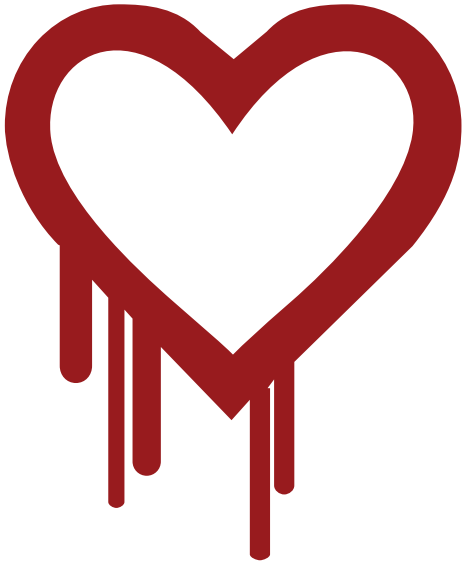
VENAFI™

Contents

Executive Summary

Venafi Labs routinely evaluates SSL/TLS vulnerabilities and has found that most Global 2000 organizations have not completely remediated Heartbleed. This leaves them vulnerable to cyber attacks, future brand damage and intellectual property loss. When the Heartbleed vulnerability was discovered in March, many organizations scrambled to patch the bug, but failed to take all of the necessary steps to fully remediate. To date, only 3% of all Global 2000 public facing services have been fully remediated following recommendations from Gartner and other industry experts.

Heartbleed Vulnerability Summary



Heartbleed takes advantage of a vulnerability in OpenSSL, whereby an attacker is able 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: Heartbleed was not just another patch-it vulnerability. It struck at the core of what creates trust online: SSL keys and certificates. If SSL keys and certificates could be compromised, websites could be spoofed for phishing attacks and encrypted communications decrypted resulting in customer data loss and intellectual property theft.

Immediately after the Heartbleed vulnerability broke experts from Bruce Schneier to Gartner's Erik Heidt made it clear that to stop Heartbleed SSL keys and certificates must be replaced. In addition to applying the OpenSSL patch, organizations would need to generate new keys, issue new certificates and revoke old certificates. Stolen keys allow websites to be impersonated and traffic to be decrypted.

The Electronic Frontier Foundation confirmed Heartbleed-related exploits occurred in November 2013, while other analyses suggest possible exploits date back two years. As a result, enterprises should assume adversaries have executed attacks using the exposed keys and certificates for some time.

Precarious Situation for Global 2000 Organizations

Venafi Labs frequently analyzes the websites of Global 2000 organizations and the Alexa Top 1 Million to identify SSL/TLS vulnerabilities. We have found that although many organizations believe they are not susceptible to Heartbleed anymore, the data shows otherwise.

Even though many Global 2000 organizations have taken basic steps to remediate Heartbleed, most have not entirely remediated this vulnerability. Venafi Labs evaluated 1639 Global 2000 organizations and found critical security flaws using the Venafi Threat Center Vulnerability Report. Only 387 G2000 organizations have fully remediated Heartbleed (See Figure 1).

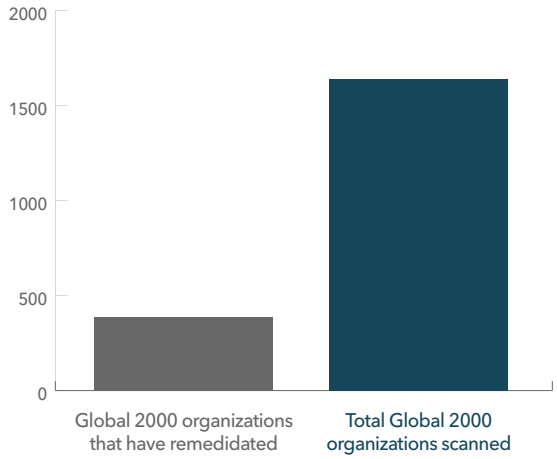


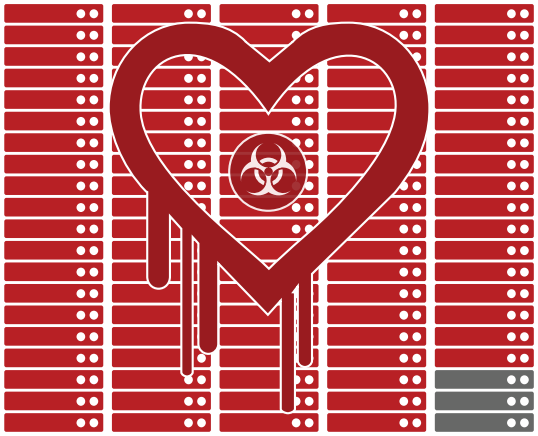
Figure 1

Venafi Labs evaluated 550,000 hosts as part of the Heartbleed scan. Venafi could confirm that over 460,000 hosts were previously or currently Heartbleed vulnerable.

Heartbleed Vulnerable
Less than one percent of hosts are confirmed to still be vulnerable to Heartbleed. No steps have been taken to patch OpenSSL on these hosts.

Remediation Incomplete (Remain Vulnerable)
Simply patching the Heartbleed vulnerability is not sufficient. It is required to also replace the private key, re-issue the certificate and revoke the old certificate. The partial remediation category consists of 449,000 hosts that have been patched against Heartbleed (97 percent of the sample size). However they have either performed 'lazy' remediation failing to replace the private key, or failed to revoke the old certificate. 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
Only 15,000 hosts total or 3 percent among all Global 2000 organizations scanned have been fully remediated from Heartbleed.



97% OF GLOBAL 2000

Organizations' external servers remain vulnerable to cyberattacks due to Heartbleed

As per Gartner, "lazy" security and OpenSSL patch management is insufficient. All keys and certificates "need to be retired and rotated."

Chart 1

The most concerning issue is there is little movement in the number of legacy, pre-Heartbleed certificates being revoked. Organizations may have patched the Heartbleed vulnerability by applying the OpenSSL patch, but remain exposed to phishing and other attacks by failing to revoke legacy certificates.

There could be a multitude of reasons as to why there is such a low revocation rate. One theory is that most certificate authorities (CAs) are not able to handle the load of the mass revocation that is required. Another is that many organizations are hesitant to revoke certificates for fear of causing a service outage on unknown systems. This in itself is concerning. Organizations should know where certificates are being used. Heartbleed has clearly highlighted the deficiencies with certificate revocation lists (CRL) and CRL distribution points (CDP) that were not designed to handle large quantities of certificate revocations.

From June to July 2014, the number of confirmed Heartbleed vulnerable sites was only reduced marginally. Heartbleed is considered to be one of the worst vulnerabilities in history and should be taken seriously.

Furthermore, there are hundreds of applications from IBM, Juniper, Cisco, and many others that are vulnerable to Heartbleed and use keys and certificates. Many of these operate behind the firewall and some may, incorrectly, assume replacing keys and certificates on these systems is not important. Assuming this would be a terrible mistake since behind-the-firewall attackers would love nothing more than to be able to spoof services like VPNs, security systems, applications servers, and more and decrypt encrypted SSL/TLS traffic.

CISOs and CIOs should not report to their CEOs, board of directors, and customers that they are safe until they've replaced all keys and certificates. Doing so is ill advised as we learn more about new exploits and the likelihood that Heartbleed exploits occurred in 2013 and before.

Enterprises must assume, just as they are with userid and passwords, that ALL keys and certificates are compromised, not just those that secured vulnerable Heartbleed systems. Kill Chain Analysis helps us understand that attackers will look to expand their attacks using similar methods and targets as their first intrusion. Further infiltration of networks means that SSL keys and certificates and SSH keys, even though not running vulnerable OpenSSL, should be assumed targets and compromised.

Respond & Remediate Now

- 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 key and certificates are in place

To help organizations respond, Venafi has prepared more guidance on remediation steps. Venafi customers have already remediated keys and certificates in hours. Venafi also recently launched it's Q3 Venafi Labs Vulnerability Report service that helps organizations identify SSL/TLS vulnerabilities for their entire publicly-facing certificate landscape at no cost. Register to generate your on-demand Venafi Labs Vulnerability Report to evaluate your organizations SSL vulnerabilities.

About Venafi

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

Part number: 1-0023-0714

info@venafi.com
Venafi.com

VENAFI™