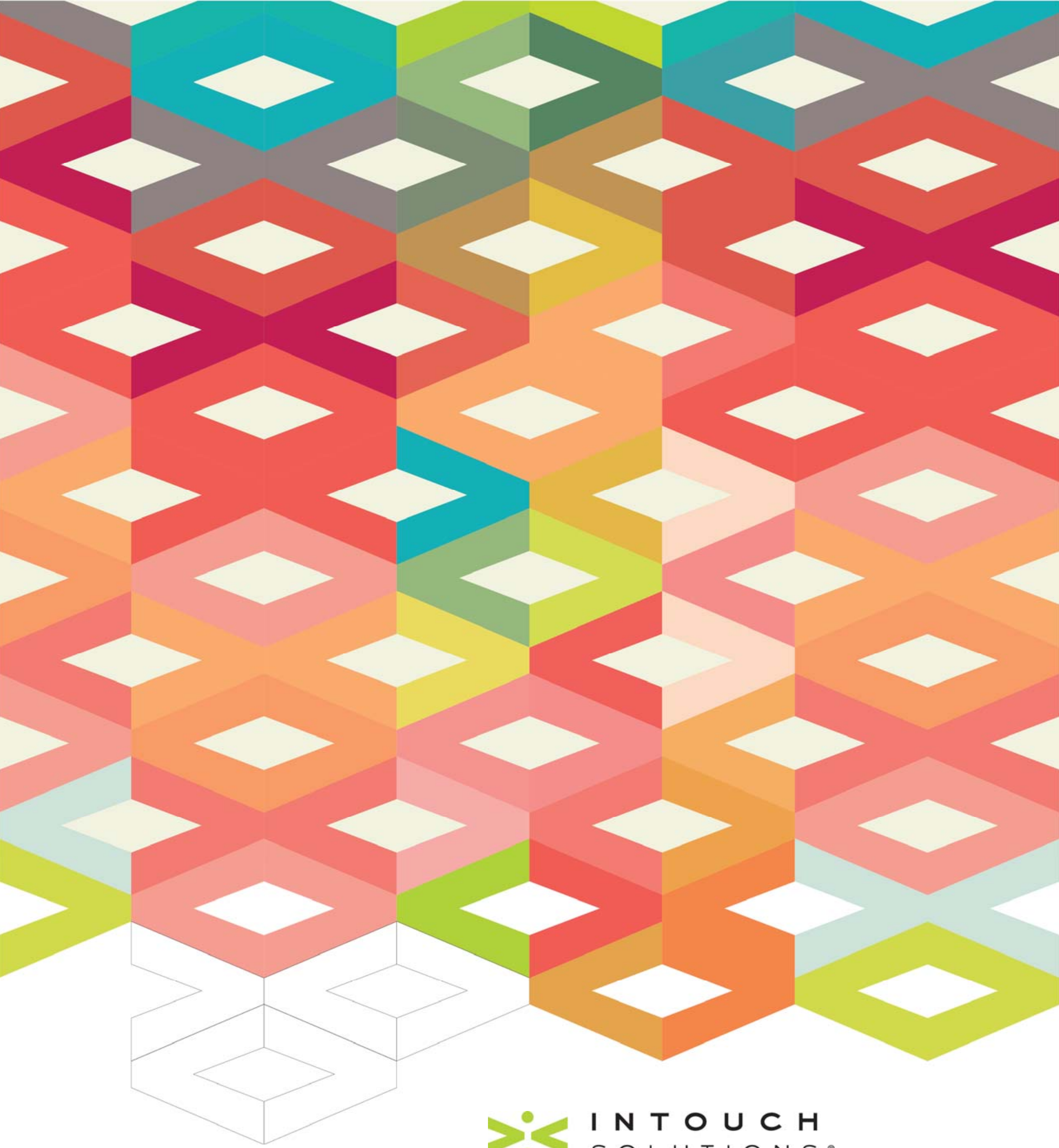

POV: THE HEARTBLEED OPENSSL VULNERABILITY

APRIL 2014

proprietary and confidential

WHAT IS THE HEARTBLEED VULNERABILITY?

In order to send and receive data securely over the Internet, web browsers use what is referred to as a secure sockets layer (SSL) to encrypt data in transit. When you use your web browser and see the padlock icon somewhere in the browser frame, this means the browser is encrypting the data being sent from your computer, mobile device or smartphone to a web server or vice versa.

Heartbleed is a security vulnerability confirmed in April 2014 that effectively weakens this data encryption for certain versions of SSL. Specifically, Heartbleed is a bug within the commonly used OpenSSL security library, utilized within the web server software, which allows Internet eavesdroppers to effectively access the keys used to encrypt the data. This means that hackers could have access to usernames, passwords, emails, and other forms of personal information by using these keys to open the SSL locks, so to speak.

It is important to note that Heartbleed only affects those open source web servers that leverage OpenSSL, primarily Apache and nginx. In turn, server operating systems that bundle these web servers, such as Ubuntu and OpenBSD, would carry the vulnerability. Heartbleed does not impact:

- Closed-source-based web server software, such as Microsoft's Internet Information Server (IIS)
- Web server software included on closed-source-based operating systems, such as Microsoft Windows or Apple OS X
- All versions of OpenSSL

If you are interested in learning more about the specific versions of OpenSSL and that are affected by Heartbleed, please see the **Appendix** for this POV. Further technical details regarding the Heartbleed bug are available at **heartbleed.com**.

HOW IS HEARTBLEED BEING MITIGATED?

Security firm Codenomicon has issued a fix for OpenSSL (OpenSSL 1.0.1g) that eliminates the underlying memory check limitation. However, it must now be applied as follows:

1. The fix is provided to operating systems vendors and appliance vendors for their incorporation into the web server software bundled with their software and firmware systems.
2. Hosting service providers need to update the appropriate web servers with these newer software versions (or apply the OpenSSL 1.0.1g patch directly) to eliminate the Heartbleed vulnerability.
3. Once the fix is applied to the appropriate web services, new SSL certificates must be requested and installed on these servers. This is required as the Heartbleed vulnerability essentially exposed the keys for the previous SSL certificates and these keys might still be in use by hackers, providing access to protected data. The Heartbleed fix addresses the root cause, but “stolen” keys still unlock secure doors.
4. Lastly, websites running on these updated web servers must force the expiration of web session keys and cookies to ensure these security containers do not contain remnants of exploited data upon a user’s next visit.

WHAT HAS INTOUCH DONE TO MITIGATE HEARTBLEED IMPACT TO OUR CLIENTS’ WEBSITES?

Intouch has determined that none of our live production servers are running Apache or nginx web servers, so these servers do not require any changes. We did determine that five of our non-production servers (essentially development servers) had Apache installed. These specific servers have been patched with the OpenSSL 1.0.1g update. Intouch will continue to monitor learnings and activity related to the Heartbleed bug and incorporate as appropriate.

WHAT DOES HEARTBLEED MEAN TO PHARMA/HEALTHCARE?

As Heartbleed essentially allows hackers to bypass security measures on otherwise secured websites or web pages, this bug leaves both PII and PHI at risk for being exploited by these hackers. This means all manner of patient information can be accessed and shared on websites, served up by the previously noted open source web servers (Apache and nginx).

Open source software is a valuable tool for solution providers in response to the diversity of business and technical challenges they are tasked with solving. The Heartbleed OpenSSL vulnerability highlights the importance of evaluating the security considerations of a solution when selecting open source software technologies. In the case of the OpenSSL defect underlying Heartbleed, the lesson is clear: Solution providers must consider the differences in rigor applied to the testing and maintenance of open source solutions as it relates to the security demands of an application.

WHAT SHOULD OUR CLIENTS DO?

Intouch recommends that our clients ensure that their web hosting providers (or internal IS partners) are aware of the Heartbleed issue and that any applicable open source production web servers (Apache or nginx) have been patched and addressed per the previously noted guidelines.

APPENDIX

WHAT VERSIONS OF OPENSSL ARE AFFECTED?

This vulnerability only affects OpenSSL versions 1.0.1 through 1.0.1f, inclusively. Versions outside this range (older and newer) are not vulnerable to Heartbleed.

WHAT WEB SERVER OPERATING SYSTEMS ARE AFFECTED?

The following operating systems, when running web server software which uses the previously noted versions of OpenSSL, are potentially vulnerable:

- Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4
- Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11
- CentOS 6.5, OpenSSL 1.0.1e-15
- Fedora 18, OpenSSL 1.0.1e-4
- OpenBSD 5.3 (OpenSSL 1.0.1c 10 May 2012) and 5.4 (OpenSSL 1.0.1c 10 May 2012)
- FreeBSD 10.0, OpenSSL 1.0.1e 11 Feb 2013
- NetBSD 5.0.2, OpenSSL 1.0.1e)
- OpenSUSE 12.2, OpenSSL 1.0.1c)

Authors: Brian Corn, Paul Pierce