How the Heartbleeds

This week on Security Now!

- XP's final 2nd Tuesday of the Month finally arrives!
- A bunch of interesting and fun miscellaneous stuff, including a MUST SEE documentary.
- A quick update on SQRL and SpinRite...
- Then full coverage of what went wrong with OpenSSL, what it means, and what to do.

Security News:

The final Second Tuesday of the Month for XP:

- Patches -- Two Critical and Two Important:
  - The BAD Microsoft Word RTF vulnerability is fixed.
  - ALL versions of Office -- definitely update Office 2003 if planning to continue.
    - (The "Fixit" no longer needed.)
  - All versions of Internet Explorer.
- "The Register": Final Windows XP Patch Tuesday will plug Word RTF vuln
  - http://www.theregister.co.uk/2014/04/04/final_winxp_patch_tuesday_pre_alert/
  - You know, the one that insta-pwns your PC when you open the file
- The Apocalypse Countdown
  - (thanks to @SimonZerafa -- first to tweet)

Enterprise Customers
Support for Windows XP
ends in: 0 : 13 : 19 : 54

- Confusion about Microsoft's Patching Policies...
  - Updates for new installations will still be available. Win2000 can still be updated.
  - So NEW updates will no longer be created, but all EXISTING updates will continue to be available.
Miscellany:

"Particle Fever"
- 8.1/10 from 211 user ratings.
- Critic's MetaScore: 87/100
- NPR (85): It's jaw-droppingly cool stuff, explained with admirable clarity by an affable physicist tour-guide, David E. Kaplan, and wedded to the tale of a massive technological undertaking like nothing in history. ("The biggest machine ever built by human beings," as one scientist puts it.) And it's flat-out thrilling.
- The Hollywood Reporter: "Particle Fever" succeeds on every level, but none more important than in making the normally intimidating and arcane world of genius-level physics at least conceptually comprehensible and even friendly to the lay viewer.
- The Globe and Mail: Their excitement is infectious and the entire endeavour is both mind-bending and tremendously human: Near the end, Peter Higgs, the recent Nobel Prize-winner and one of the scientists who first predicted the particle back in 1964, is seen in Switzerland watching the data results come in, while a tear trickles down his cheek.
- [http://particlefever.com/](http://particlefever.com/) (thanks Simon!)

"Rogue Code" - by Mark Russinovich
- Available now for Kindle / Preorder Hardcopy.
- A Jeff Aiken Novel (Jeff Aiken Series)
- "Trojan Horse" and "Zero Day"
- A fictionalized "Security Now!" podcast... and then some.

SlySoft DVD decryption tools.
- "AnyDVD" / Wikipedia:
  - AnyDVD is a Microsoft Windows driver allowing decryption of DVDs on-the-fly, as well as targeted removal of copy preventions and user operation prohibitions (UOPs). With an upgrade, it will also do the same for HD DVD and Blu-ray Disc. The AnyDVD program runs in the background, making discs unrestricted and region-free. In addition to removing digital restrictions, AnyDVD will also defeat Macrovision analog copy prevention. (AnyDVD will not work on VHS tapes, only discs.[4]) Analog prevention distorts the video signal to prevent high quality copying from the output. AnyDVD is also able to remove copy-prevention from audio CDs.
Snowden:

- I DO understand that Snowden doesn't control specific disclosures any longer.
- He's RESPONSIBLE inasmuch as he was the original source for his leaks.
- (Though the NYT said that their data was not from Snowden, while explicitly referring to him.)
- My annoyance was over the whole enterprise.
- Non-US people felt that it wasn't about the 4th amendment, but Snowden is a US citizen and past US contractor employee... and the NSA is, of course, a creation of the US Congress.
"PushBullet"
- Don Houle @therealdonhoule
- @SGgrc Check out Pushbullet for getting data to/from PC and i-devices.
- http://bit.ly/1j4XDFi (Appears to be a Google tool?). Enjoy!
- https://www.pushbullet.com

Cold Drip Brewing via Kickstarter

SQRL:
- With the additions of Lithuanian & Latvian... we’re now at 54 languages!
- 362 participants.
- Now: Harvesting Entropy

SpinRite:
Sean McCormack @seanmmccormack
Thank you @SGgrc! http://pic.twitter.com/F4yFhkPngo
How the Heartbleeds


OpenSSL Security Advisory [07 Apr 2014]

========================================
TLS heartbeat read overrun (CVE-2014-0160)
========================================

A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64k of memory to a connected client or server.

Only 1.0.1 and 1.0.2-beta releases of OpenSSL are affected including 1.0.1f and 1.0.2-beta1.

Thanks for Neel Mehta of Google Security for discovering this bug and to Adam Langley <agl@chromium.org> and Bodo Moeller <bmoeller@acm.org> for preparing the fix.

Affected users should upgrade to OpenSSL 1.0.1g. Users unable to immediately upgrade can alternatively recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS.

1.0.2 will be fixed in 1.0.2-beta2.

The TOR Project summed it up:


A new OpenSSL vulnerability on 1.0.1 through 1.0.1f is out today, which can be used to reveal memory to a connected client or server.

If you're using an older OpenSSL version, you're safe.

Note that this bug affects way more programs than just Tor — expect everybody who runs an https webserver to be scrambling today. If you need strong anonymity or privacy on the Internet, you might want to stay away from the Internet entirely for the next few days while things settle.

Here are our first thoughts on what Tor components are affected:

Clients: Tor Browser shouldn't be affected, since it uses libnss rather than openssl. But Tor clients could possibly be induced to send sensitive information like "what sites you visited in this session" to your entry guards. If you're using TBB we'll have new bundles out shortly; if you're using your operating system's Tor package you should get a new OpenSSL package and then be sure to manually restart your Tor.
Relays and bridges: Tor relays and bridges could maybe be made to leak their medium-term onion keys (rotated once a week), or their long-term relay identity keys. An attacker who has your relay identity key can publish a new relay descriptor indicating that you're at a new location (not a particularly useful attack). An attacker who has your relay identity key, has your onion key, and can intercept traffic flows to your IP address can impersonate your relay (but remember that Tor's multi-hop design means that attacking just one relay in the client's path is not very useful). In any case, best practice would be to update your OpenSSL package, discard all the files in keys/ in your DataDirectory, and restart your Tor to generate new keys.

Hidden services: Tor hidden services might leak their long-term hidden service identity keys to their guard relays. Like the last big OpenSSL bug, this shouldn't allow an attacker to identify the location of the hidden service, but an attacker who knows the hidden service identity key can impersonate the hidden service. Best practice would be to move to a new hidden-service address at your convenience.

Directory authorities: In addition to the keys listed in the "relays and bridges" section above, Tor directory authorities might leak their medium-term authority signing keys. Once you've updated your OpenSSL package, you should generate a new signing key. Long-term directory authority identity keys are offline so should not be affected (whew). More tricky is that clients have your relay identity key hard-coded, so please don't rotate that yet. We'll see how this unfolds and try to think of a good solution there.

Tails is still tracking Debian oldstable, so it should not be affected by this bug.

Orbot looks vulnerable; we'll try to publish more details here soon.

It looks like most of the webservers in the https://www.torproject.org/ rotation need upgrades too, and maybe we'll need to throw away our torproject SSL web cert and get a new one — hopefully we'll deal with all that soon.

Ars Technica

<quote> Researchers have discovered an extremely critical defect in the cryptographic software library an estimated two-thirds of Web servers use to identify themselves to end users and prevent the eavesdropping of passwords, banking credentials, and other sensitive data. Default SSL package used by Apache... as well as just about everything else that's not Microsoft-based.

<quote> The bug, which has resided in production versions of OpenSSL for more than two years, could make it possible for people to recover the private encryption key at the heart of the digital certificates used to authenticate Internet servers and to encrypt data traveling between them and end users. Attacks leave no traces in server logs, so there's no way of knowing if the bug has been actively exploited. Still, the risk is extraordinary, given the ability to disclose keys, passwords, and other credentials that could be used in future compromises.
The researchers, who work at Google and software security firm Codenomicon, said even after vulnerable websites install the OpenSSL patch, they may still remain vulnerable to attacks. The risk stems from the possibility that attackers already exploited the vulnerability to recover the private key of the digital certificate, passwords used to administer the sites, or authentication cookies and similar credentials used to validate users to restricted parts of a website. Fully recovering from the two-year-long vulnerability may also require revoking any exposed keys, reissuing new keys, and invalidating all session keys and session cookies.


OpenSSL is by far the Internet's most popular open-source cryptographic library and TLS implementation. It is the default encryption engine for Apache, nginx (pronounced "engine-x"), which according to Netcraft runs 66 percent of websites. OpenSSL also ships in a wide variety of operating systems and applications, including the Debian Wheezy, Ubuntu, CENTOS, Fedora, OpenBSD, FreeBSD, and OpenSUSE distributions of Linux. The missing bounds check in the handling of the Transport Layer Security (TLS) heartbeat extension affects OpenSSL 1.0.1 through 1.0.1f.

So... Can it be exploited? The researchers who discovered it wrote:

"We attacked ourselves from outside, without leaving a trace. Without using any privileged information or credentials, we were able steal from ourselves the secret keys used for our SSL certificates, user names and passwords, instant messages, emails and business critical documents and communication."

Writes Dan: They called on white-hat hackers to set up "honeypots" of vulnerable TLS servers designed to entrap attackers in an attempt to see if the bug is being actively exploited in the wild.

Heatbeat CAN be disabled in OpenSSL through a recompile... but then you might as well update to 1.0.1g.

Good coverage at: http://heartbleed.com/

History:
- v0.9.8 / July 5, 2005
- v1.0.0 / March 29, 2010
- v1.0.1 March 14, 2012
  - Successor of 1.0.0h
  - Supports TLS v1.2
  - SRP support
  - TLS "Heartbeat" RFC 6520 / February 2012
  - TLS is based on reliable protocols, but there is not necessarily a feature available to keep the connection alive without continuous data transfer. The Heartbeat Extension as described in this document overcomes these limitations. The user can use the new HeartbeatRequest message, which has to be answered by the peer with a HeartbeatResponse immediately.
- v1.0.1g - Now available
- v1.0.2 - in beta release, coming soon.
Netcraft:

The Code Diff:
https://github.com/openssl/openssl/commit/96db9023b881d7cd9f379b0c154650d6c108e9a3
http://pastebin.com/5PP8JvqA

Analysis of the bug:
(with thanks to @e_StrategyPro)

The first early "Heartbleed" test service:
http://filippo.io/Heartbleed
I’d use SSLLabs.com for online, but Filippo Valsorda has a command-line version on Github.
https://github.com/FiloSottile/Heartbleed
Ivan Ristic tweeted:
Up to 30% of the servers in the SSL Pulse data set support TLS 1.2. Most of them are probably vulnerable to the OpenSSL heartbeat bug.

Ivan and I have been corresponding since the news. I’m sure he didn’t need my urging to add “Heartbleed” support. But he wrote this morning to notify me that it was already online: [https://www.ssllabs.com/](https://www.ssllabs.com/)

GRC.COM’s report at SSL Labs. Note first green box.

The Lastpass Blog

Netcraft:

Make sure your servers check for revoked certificates!