OpenSSL after HeartBleed

Tim Hudson
Cryptsoft, OpenSSL Team

Rich Salz
Akamai Technologies, OpenSSL Team
The most important date

• April 3, 2014
The most important date

- April 3, 2014
- HeartBleed
- Re-key the Internet
So what was HeartBleed?

- Massive mainstream press coverage
So what was HeartBleed?

- A very simple bug, the code didn’t check a buffer length.

So what was HeartBleed?

To the best of our knowledge, Heartbleed is the first computer systems bug to have both its own website and its own logo, the cute bleeding heart. As such, Heartbleed sets a precedent that will have both positive and negative ramifications for future vulnerabilities and malware.

...

Even among the vast majority of the population who have no idea what OpenSSL is, people everywhere quickly found out that a major bug could compromise their Internet security.

The sky is falling …

- **CVE-2011-0014** - infoleak, true impact unknown
- **CVE-2012-2110** - possibly arbitrary code execution on reading certificates
- **CVE-2012-2333** - buffer over-read, true impact unknown
- **CVE-2014-1266** - “goto fail” server spoofing (Apple)
- **CVE-2014-0160** - Heartbleed
- **CVE-2014-0224** - “early CCS” disables encryption
- **CVE-2014-1568** - RSA signature forgery (NSS)
Or is it ...
So what was HeartBleed?

• Basically missed validating a variable containing a length
• Contributed code had a bug – bug was in code base for three years!
• Project team member review missed the bug
• Other team members either didn’t review or also simply missed the bug
• Multiple external security reviewers and auditors missed the bug
• OpenSSL external developers and users missed the bug
• Security review teams in major OpenSSL using organisations missed the bug
• All existing code analysis tools missed the bug
• Bug allowed clients to attack servers and servers to attack clients
So what was HeartBleed?
Life before HeartBleed

• Project had effectively become somewhat moribund
• Releases were not pre-announced, no documented policies
• Source code was complex and arcane
• Hard to maintain; harder to contribute
• Main developers were overworked and overcommitted
• Project donations minimal (sub USD$2000 per annum)
Repo activity, 2012 - 2014

Contributions to master, excluding merge commits

OpenSSL
Cryptography and SSL/TLS Toolkit

LinuxCon/Europe 2016
How did we let this happen?

• Very little time spent on building community
• Long lead time to understand code
• Static project team membership
• Need to focus on consulting dollars (FIPS140) to keep project alive
• No ability to make, announce, and keep to plans

• ... all added up to “ultra cautious” to any change attitude
The usual questions ...

• How could the project let this happen?
• How could the project members be so stupid?
• What other nasty break-the-internet bugs are yet to be found?
• Why didn’t the project fix this sooner?
• Why didn’t all those companies making money off OpenSSL contribute?
• How could we possibly trust the team to not make the same mistake in future?
• Why shouldn’t I simply switch over to one of the forks?
After-affects

• Wider recognition of dependency on critical under-funded projects

• Creation of the Core Infrastructure Initiative, a multi-million dollar effort to add effective resources to the open source projects that make the Internet work
Growing the Team

• Prior to April 2014
  – Two main developers (one primary committer) entirely on volunteer basis; all other team members focused on other areas; main developer basically funded by paid OpenSSL consulting work
  – No formal decision making process

• As of December 2014
  – Fifteen project team members; a couple inactives
  – Two full time funded by CII; two full time funded by donations
  – Formal decision making process
After-affects

• We had the first-ever F2F
• Drafted major policies:
  – Release strategy
  – Security policy
  – Coding style
• Socialized with each other; POODLE helped
Transparency

• We use GitHub for many things.
• We have public policies for security fixes, a release schedule and high-level content, code of conduct, and so on.
• Email traffic increased, and (seems) more useful
2016 Activity (so far)

• 3246 commits

• One major release, 15 bugfix releases; 29 CVE’s

• GitHub:
  – 281 users created 122 issues, 63 PR’s.
  – Team closed 972 issues; 733 PR’s (usually merged)
Repo Activity, 2014-2016
Transparency: security fixes

Source: OpenSSL Blog Entry

LinuxCon/Europe 2016
Bug tracking
Project Supported Releases

- Version 1.1.0 will be supported until 2018-04-30.
- Version 1.0.2 will be supported until 2019-12-31 (LTS).
- Support for version 1.0.1 will cease on 2016-12-31. No further releases of 1.0.1 will be made after that date. Security fixes only will be applied to 1.0.1 until then.
- Version 1.0.0 is no longer supported.
- Version 0.9.8 is no longer supported.
Renewed focus

• Security researchers more actively looking for issues
• More fuzz testing going on
• Increased focus on automated testing
• Static code analysis tools rapidly updated
• Reported issues more quickly analyzed
• **Mandatory team member code reviews**
Project Roadmap

• Roadmap has been published and progress against roadmap updated - https://www.openssl.org/policies/roadmap.html
• Major items:
  – clear bug backlog
  – documentation
  – complexity
  – coding style
  – code reviews
  – release plan
  – platform strategy
  – security strategy
Vitality is its own reward

Daniel Stenberg @bagder · 18m
I filed a crash bug to #OpenSSL, got a fix and verified it - within 15 minutes! The fix: github.com/openssl/openssl...

View summary

sbagmeijer commented 17 minutes ago

@levitte no worries if you want me to try something else to make sure the perl works let me know.

I really appreciate the quick response now I can release the 1.1.0 Alpha 2 rpm this evening :).
Future Plans

• TLS 1.3
• Apache v2 license
• More testing
• FIPS

• ... what else is needed?
FIPS140

• FIPS140 related work effectively entirely funded the OpenSSL project for the last five years
• Selling into USA Government where FIPS140-2 support is mandatory is important to most large vendors
• The validation process is time consuming and subject to changed requirements
• Coordinating multiple sponsors on a multi-year journey with no guarantee of successful outcome is in itself challenging
07/09/12: Added SW 2.0.1, Alg Carts AES 2116, DRBG 229, OSA 661, HMAC 1288, RNG 1087, RSA 1086, SHA 1840, TDES 1346, EOSA 315, and OUI. 24. Replaced Cascade Server with CascadeOS. Added OEs Apple iOS 5.1 (gcc Compiler Version 4.2.1); Microsoft Windows CE 6.0 (Microsoft C++) Optimizing Compiler Version 15.00 for ARM; Microsoft Windows CE 5.0 (Microsoft C++) Optimizing Compiler Version 13.10 for ARM; Linux 2.6 (gcc Compiler Version 4.1); DSP Media Framework 1.4 (TSM320C64x+C Compiler Version 6.0.13); Android 4.0 running on Ti OMAP 3 (ARMv7) with NEON (gcc Compiler Version 4.4.3); updated security policy.
07/18/12: Updated security policy.
10/12/12: Added SW 2.0, Alg Carts AES 2234, DRBG 264, OSA 693, HMAC 1363, RNG 119, RSA 1145, SHA 1923, TDES 1398, EOSA 347 and OUI. 36 and updated security policy plus added OE NotBID 5.1 (gcc Compiler Version 4.1.3).
01/12/13: Updated contact phone number and added Microsoft Windows 2008 running on Intel Xeon E3-1220v2 (32-bit) (Microsoft 32-bit C++ Optimizing Compiler Version 16.00 for x64); RHLS 6 running on Intel Xeon E3-1220v2 (32-bit) (gcc Compiler Version 4.4.1); RHLS 6 running on Intel Xeon E3-1220v2 (64-bit) (gcc Compiler Version 4.4.6); Microsoft Windows 7 running on Intel Core i5-2430M (64-bit) with AES-NI (Microsoft C++) Optimizing Compiler Version 16.00 for x64) and updated security policy.
02/06/13: Added "*" under viphere** for some OE and updated security policy.
07/02/13: Added algorithm ECSA 378, RVF 49 plus Android 4.1 and 4.2 and updated security policy.
02/08/13: Added SW 2.0.3, Alg Carts AES 2342, DRBG 292, OSA 734, HMAC 1451, RNG 1166, RSA 1205, SHA 1929, TDES 1465, EOSA 383 and OUI. 53 and updated security policy plus added OWE Embedded Compact 7 running on Freescale i.MXS36X (ARMv7) with NEON (Microsoft C++) Optimizing Compiler Version 15.00.20720); Windows Embedded Compact 7 running on Freescale i.Mxs36X (ARMv7) with NEON (gcc Compiler Version 4.4.6); Apple iOS 4.0 running on Qualcomm Snapdragon APQ8060 (ARMv7) with NEON (gcc Compiler Version 4.4.3).
08/02/13: Added OE and OWE VMware Horizon Mobile 1.3 under VMware running on Fervicim XI.MXS36X (ARMv7) with NEON (gcc Compiler Version 4.4.6); Samsung CLX-2160FN (ARMv7) with NEON (gcc Compiler Version 4.4.5) and updated security policy.
07/18/13: Updated security policy adding a logo of a sponsor.
10/08/13: added new OE: Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) with NEON (gcc Compiler Version 4.7.3); Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) with NEON (gcc Compiler Version 4.7.3); Linux 3.8 running on ARM Cortex A9 (ARMv7) with NEON (gcc Compiler Version 4.7.3) and updated security policy.
09/27/13: Added new OE: Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) with NEON (gcc Compiler Version 4.7.3); Ubuntu 13.04 running on AM335x Cortex-A8 (ARMv7) with NEON (gcc Compiler Version 4.7.3) and updated security policy.
06/27/14: Added SW 2.0.6, added Algorithm certs AES 2348, DRBG 342, OSA 764, HMAC 1262, RNG 1203, RSA 1273, SHA 2102, Triple-OES 1322, EOSA 413 and OUI. 85, added QNX 6.4 running on Freescale i.MX25 (ARMv4) (gcc Compiler Version 4.3.3); Apple iOS 6.1 running on Apple A6x Soc (ARMv7) (gcc Compiler Version 4.2.1); iOes 3 running on Freescale i.MX627 (ARMV7TE) (gcc Compiler Version 4.3.2) and updated security policy.
08/16/14: added new OE: VMware Horizon Workspace 2.1 under viphere running on Intel Xeon E3-1220 with AES-NI (gcc Compiler Version 4.5.1); VMware Horizon Workspace 1.5 under viphere running on Intel Xeon E3-1220 with AES-NI (gcc Compiler Version 4.5.1) and updated security policy.
10/12/14: added new OE: Android OS 1.0 under viphere running on Intel Xeon E3-1220 with AES-NI (gcc Compiler Version 4.6.3); PixelOS 1.0 under viphere running on Intel Xeon E3-2430 (64-bit) with AES-NI (gcc Compiler Version 4.6.3) and updated security policy.
06/27/14: Added SW 2.0.6 and updated the security policy.
07/03/14: Added SW 2.0.7, AES 2824, DRBG 445, OSA 853, HMAC 1768, RNG 1278, RSA 1477, SHA 2388, Triple-OES 1695, EOSA 496, CVF 260, OUI. Linux 2.6 running on Freescale s5dh02 (PPC) (gcc Compiler Version 4.4.1); AcornOS 1.0 running on Intel Core i7-3670QF (x64) without AES-NI (gcc Compiler Version 4.6.2); AcornOS 1.0 running on Intel Core i7-3670QF (x64) with AES-NI (gcc Compiler Version 4.6.2); FreeBSD 8.4 running on Intel Xeon E5440 (x64) without AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.1 running on Xeon X5430L (x64) without AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.1 running on Xeon X5430L (x64) with AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.1 running on Xeon X5430L (x64) with AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.2 running on Xeon X5430L (x64) without AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.2 running on Xeon X5430L (x64) with AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.2 running on Xeon X5430L (x64) with AES-NI (gcc Compiler Version 4.2.1) and updated the security policy.
09/02/14: Added OE AOKOS 5.3 running on Xeon E5640 (x64) without AES-NI (gcc Compiler Version 4.2.1); FreeBSD 9.2 running on Xeon X5430L (x64) with AES-NI (gcc Compiler Version 4.2.1) and updated the security policy.
10/16/14: Added OE FreeBSD 8.4 running on Intel Xeon E5440 (x64) 32-bit (gcc Compiler Version 4.2.1) and updated the security policy.
12/14/14: Added SW 2.0.9, AES 5090, DRBG 607, OSA 896, HMAC 1937, RNG 1314, RSA 1581, SHA 2553, Triple-OES 1780, EOSA 558, CVF 372, OWE VMware Horizon Workspace 2.1 under viphere running on Freescale i.MX52 (ARMv4) (gcc Compiler Version 4.5.1); QNX 6.5 running on Freescale i.MX52 (ARMv4) (gcc Compiler Version 4.3.3); Apple iOS 7.1.6 running on Apple A7 (ARMv8) without AES-NI (clang Compiler Version 3.5); FreeBSD 10.0 running on Intel X86-64, (x64) with AES-NI (clang Compiler Version 3.5) and updated security policy.
11/25/15: Removed incomplete platforms listings from OE.
09/04/16: Added SW 2.0.10, AES 3264, DRBG 723, OSA 933, HMAC 2063, RNG 1349, RSA 1664, SHA 2702, Triple-OES 1853, EOSA 620, CVF 472, updated several OE and updated the security policy.

Degradation use of the non-approved RNG.

Updated vendor name.
FIPS140 Plans

• The OpenSSL FIPS 2.0 module works with OpenSSL-1.0.x
• The previous OpenSSL FIPS 1.0 module for OpenSSL-0.9.x is no longer usable
• New FIPS module coming:
  – Thanks to SafeLogic for funding!
  – Will work with 1.1.0
  – Major goal is to make the FIPS changes “less intrusive”
Major Lessons

• Relying on any single individual to perform superhuman feats ultimately results in disappointment
• Code reviews actually require the reviewers to review the code in detail
• Assuming that users will review code is clearly a flawed strategy
• Assuming that automated code analysis tools by themselves can completely replace experienced code reviews is incorrect
How to Contribute

• Download the pre-releases and build your applications
• Help is a two-way street, join the virtuous circle. Or at least join the openssl-dev and/or openssl-users mailing lists
• Report bugs through RT, submit patches on GitHub. Help close bugs.
• If you are doing more than TLS for HTTP, please let us know
• More ideas on the Community page of www.openssl.org
The OpenSSL Development Team

- Matt Caswell (UK)*#  
- Mark Cox (UK)*  
- Viktor Dukhovni (US)  
- Steve Henson (UK)#  
- Tim Hudson (AU)*  
- Lutz Jänicke (DE)*  
- Emilia Käsper (CH)*  
- Ben Laurie (UK)  
- Richard Levitte (SE)*#  
- Steve Marquess (US)*

- Bodo Möller (CH)  
- Andy Polyakov (SE)*#  
- Kurt Roeckx (BE)*  
- Rich Salz (US)*  
- Geoff Thorpe (CA)

Total: AU, BE, CA, CH(2), DE, SE(2), UK(4), US(3)

* means here at LinuxCon  
# means funded (by OpenSSL or CII)
Questions?