
black hat
USA 2014
EPIDEMIOLOGY OF SOFTWARE VULNERABILITIES: A STUDY OF ATTACK SURFACE SPREAD
Kymberlee Price
@Kym_Possible
Director of Strategic Operations
Synack
Jake Kouns
@jkouns
CISO
Risk Based Security


UNDER PRESSURE


DEADLINE


BETTER
FASTER
CHEAPER

what am I

forgetting?

Hint! security

Development Realities

Can only pick two!

Third-Party Libraries To The Rescue

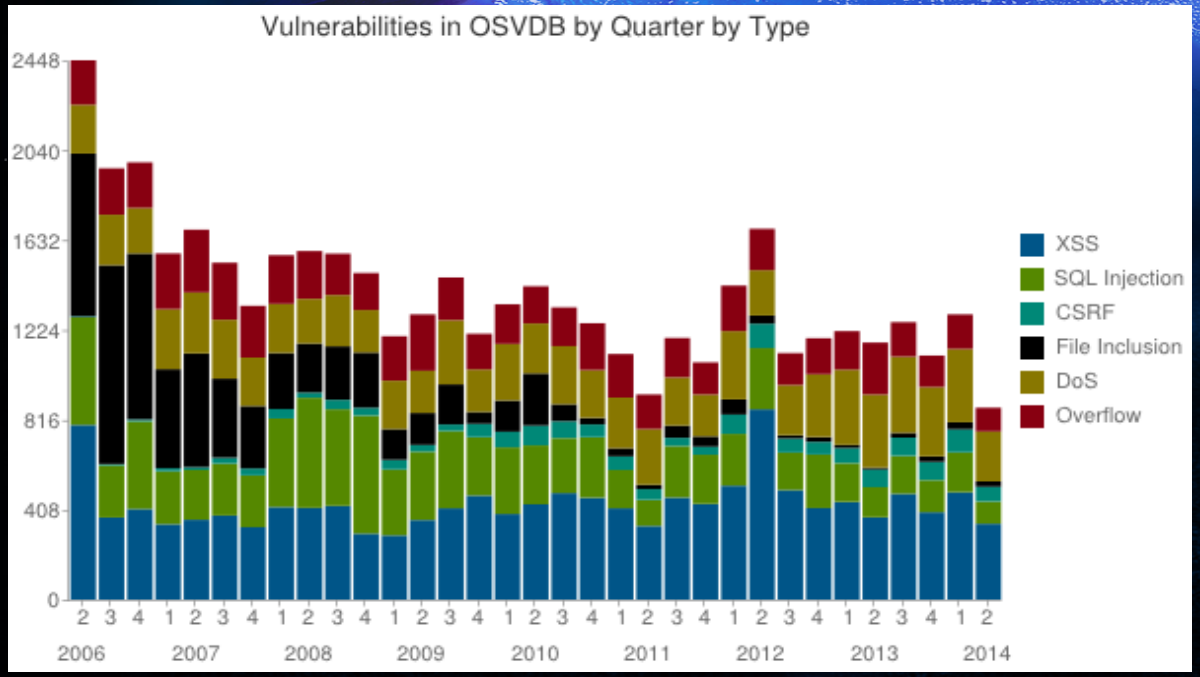
- Developers using established third-party libraries to
  - Speed up the development process
  - Realize quality improvements over creating an in-house proprietary solution from the ground up.


black hat
USA 2014
SO WHAT IS THE PROBLEM?

Where The Vulns Are

"When reviewing this report, you find that it is flawed and not referring to 3rd Party Libraries. But rather from third party – i.e. – non-Microsoft – programs.

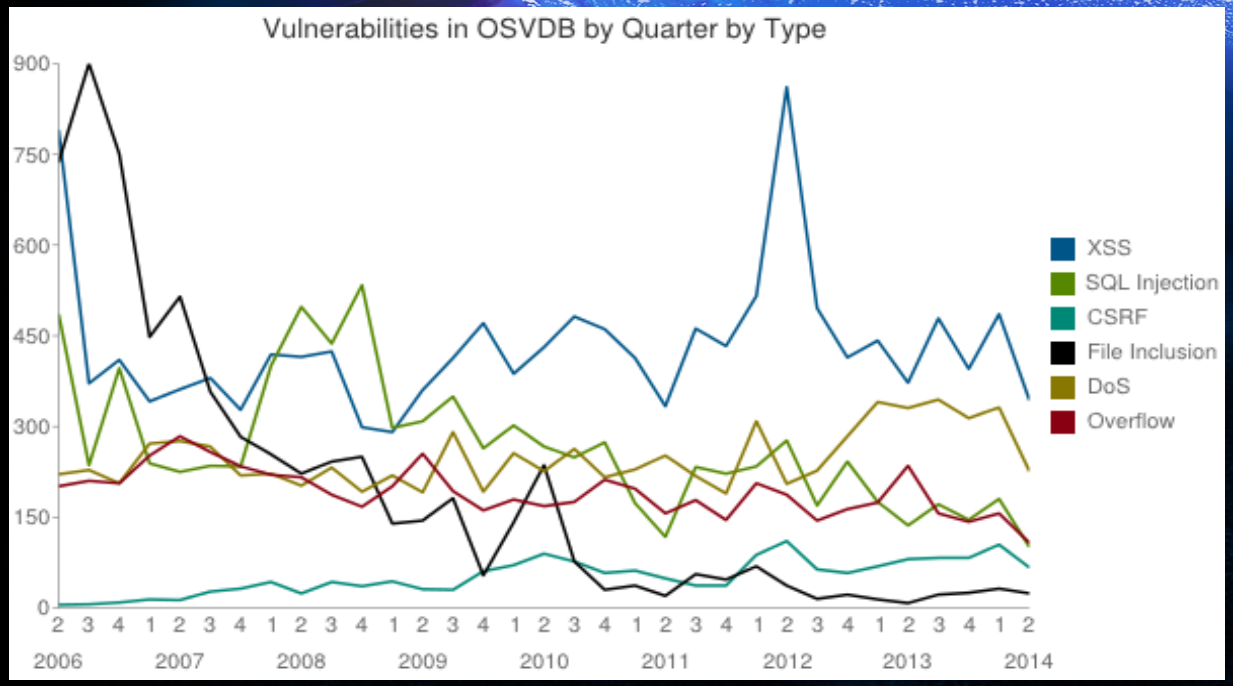
Vulnerabilities by Type



2014: 5,027
2013: 10,868
2012: 10,205
2011: 7,852
2010: 9,110
2009: 8,147
2008: 9,740
2007: 9,559
2006: 11,029

Source: OSVDB.org
*YTD June 2014

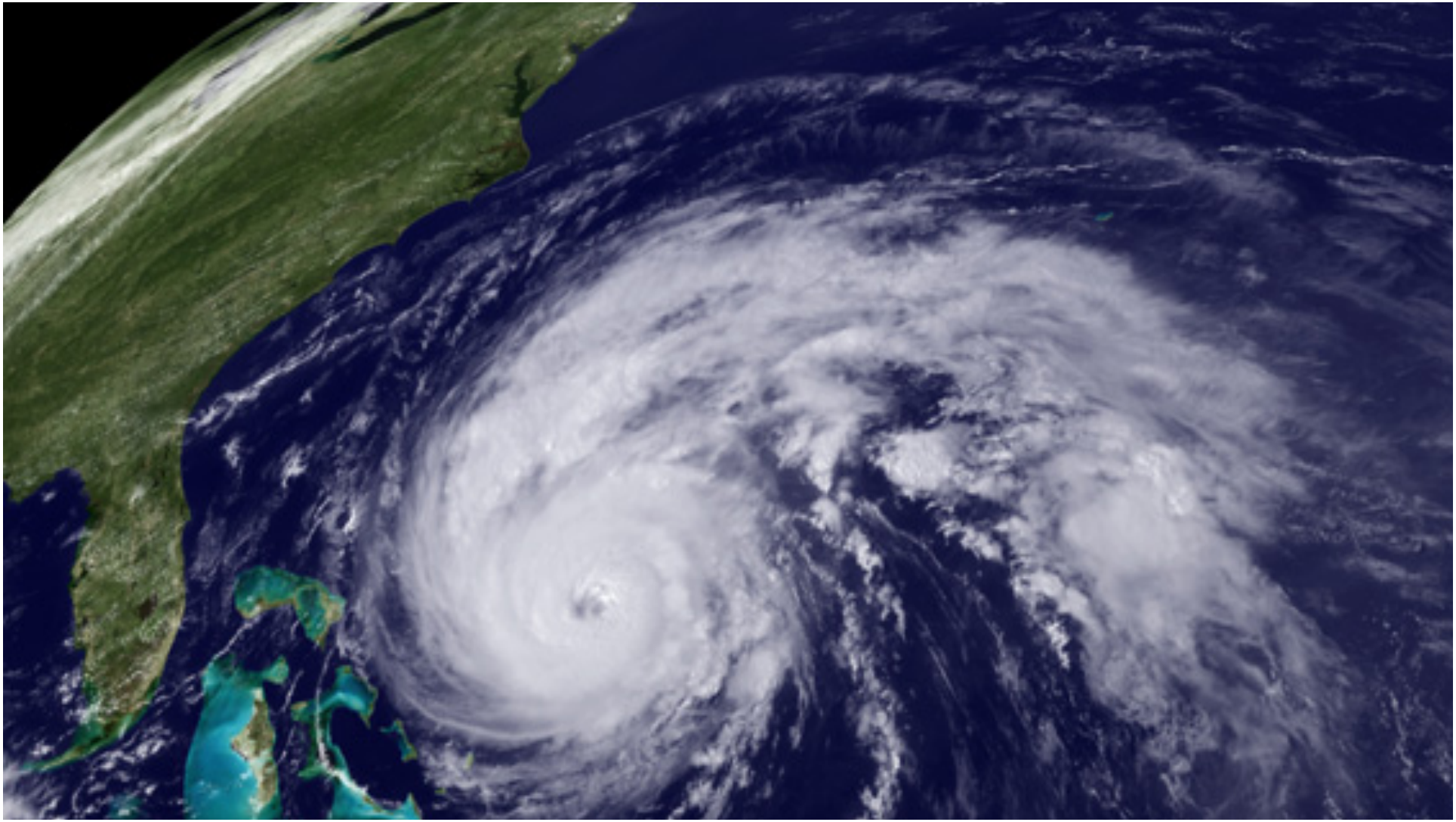
Vulnerabilities by Type

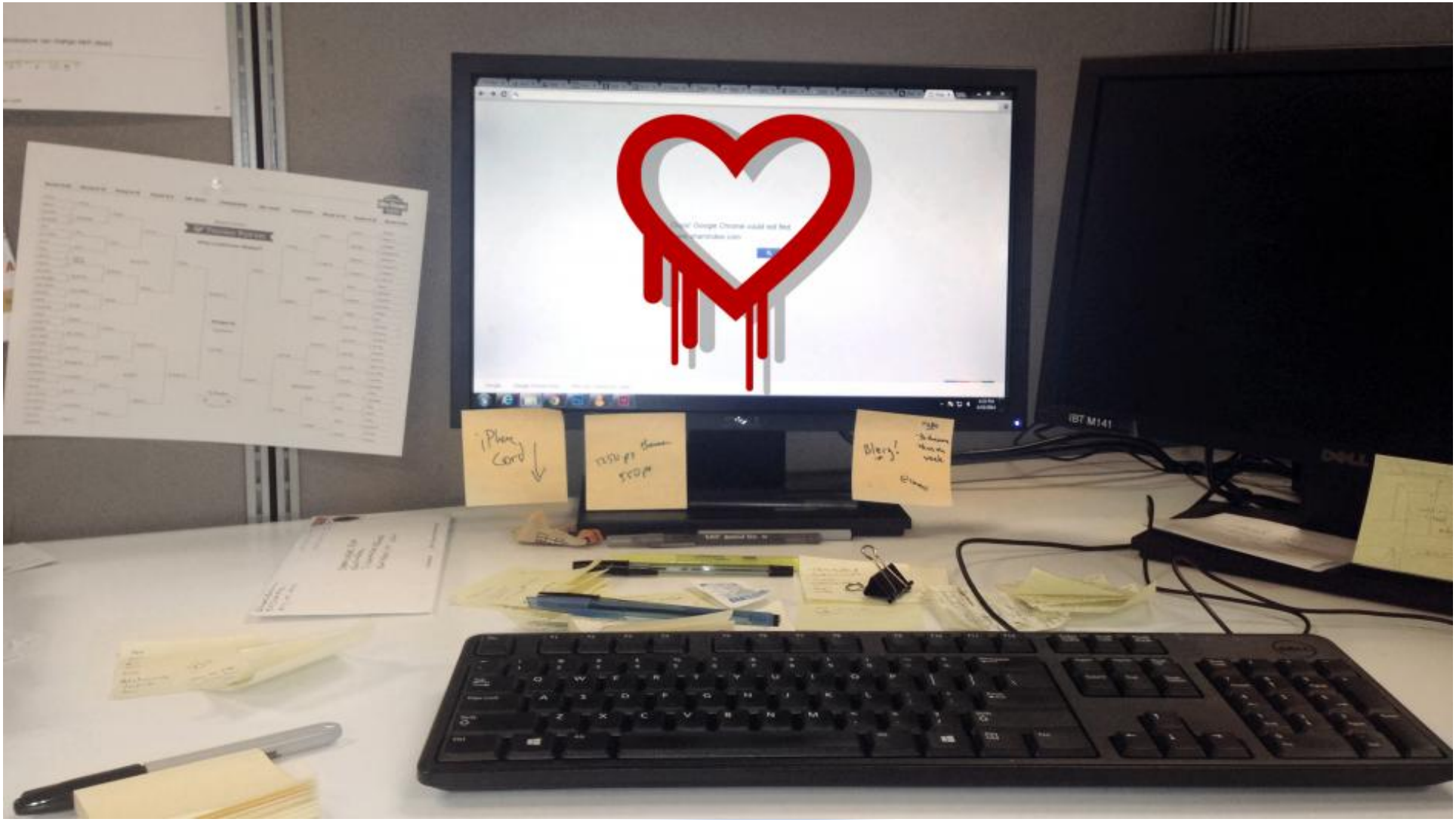


2014: 5,027
2013: 10,868
2012: 10,205
2011: 7,852
2010: 9,110
2009: 8,147
2008: 9,740
2007: 9,559
2006: 11,029

Source: OSVDB.org
*YTD June 2014


USA 2014




iPhone Cord
Bleary!
IBT M141

Estimated 100+ Vendors

impacted by Heartbleed

Vendor's Impacted By HeartBleed

SECURITY heartbleed, security

Two months later, Heartbleed patching stalls out with 300k servers still vulnerable

Ian Paul
@ianpaul

Jun 23, 2014 7:04 AM

The Heartbleed bug may be a devastating flaw still affecting thousands of websites, but efforts to patch any remaining systems are effectively over.

Two months after Heartbleed surfaced in April, more than 300,000 unpatched servers remain vulnerable to Heartbleed. The figure comes from Errata Security's Robert Graham who recently scanned the Internet for a third time to get a count of Heartbleed-vulnerable sites

Efficiency At What Cost?

- Not just one library impacting many organizations
- A single application may have as many as 100 different third party libraries implemented
  - That is a whole lot of patching to keep up on for both devs and customers


black hat
USA 2014
LETS TALK DATA

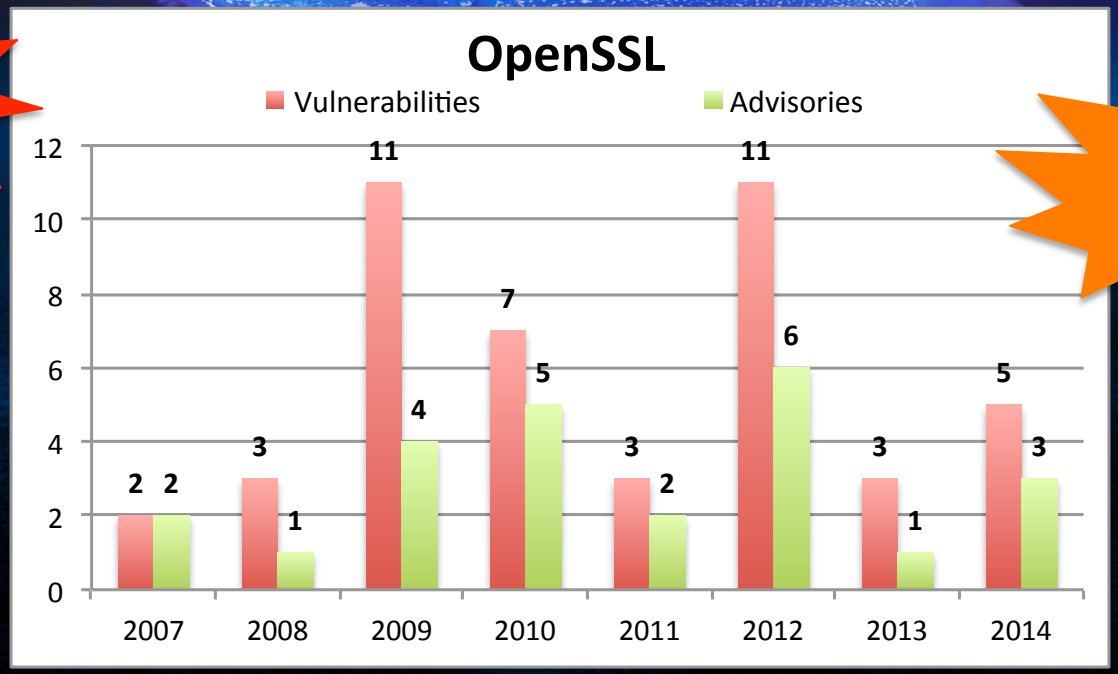
Biggest Offenders

- What libraries are the biggest offenders for spreading pestilence?
  - Volume of vulnerabilities 2007-2014
  - Frequency of release 2007-2014
  - Average vulnerability severity
  - Pervasiveness of library usage

OpenSSL

Cryptography and SSL/TLS Toolkit

45 Vulns



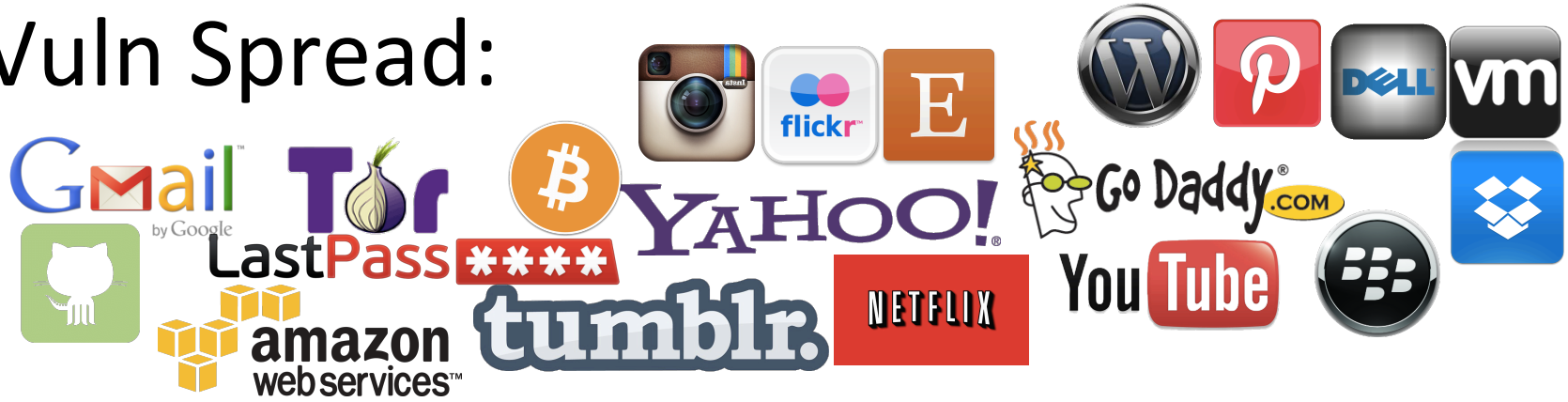
1-6 releases per year

Average CVSS 5.39

black hat USA 2014

OpenSSL™
Cryptography and SSL/TLS Toolkit

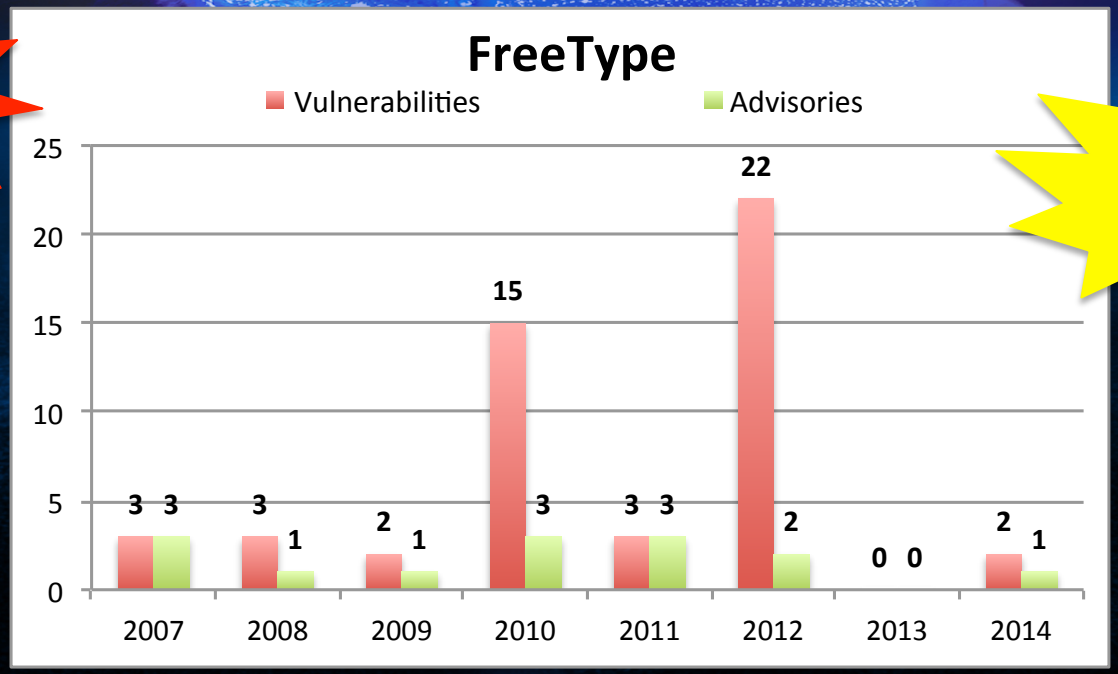
Vuln Spread:



…And multiple products by HP, Oracle (including Java), F-Secure, IBM, MySQL, Novell, OpenBSD, Intel, Juniper, Rapid7, nginx, Huawei, Trend Micro, Linux, Tableau, McAfee, F5, Cisco, Fortinet, Sophos, Python, Citrix, SUSE, Ubuntu, Debian, FreeBSD, RedHat…

the FreeType Project

50 Vulns



2 releases per year

Average CVSS 7.89

black hat USA 2014

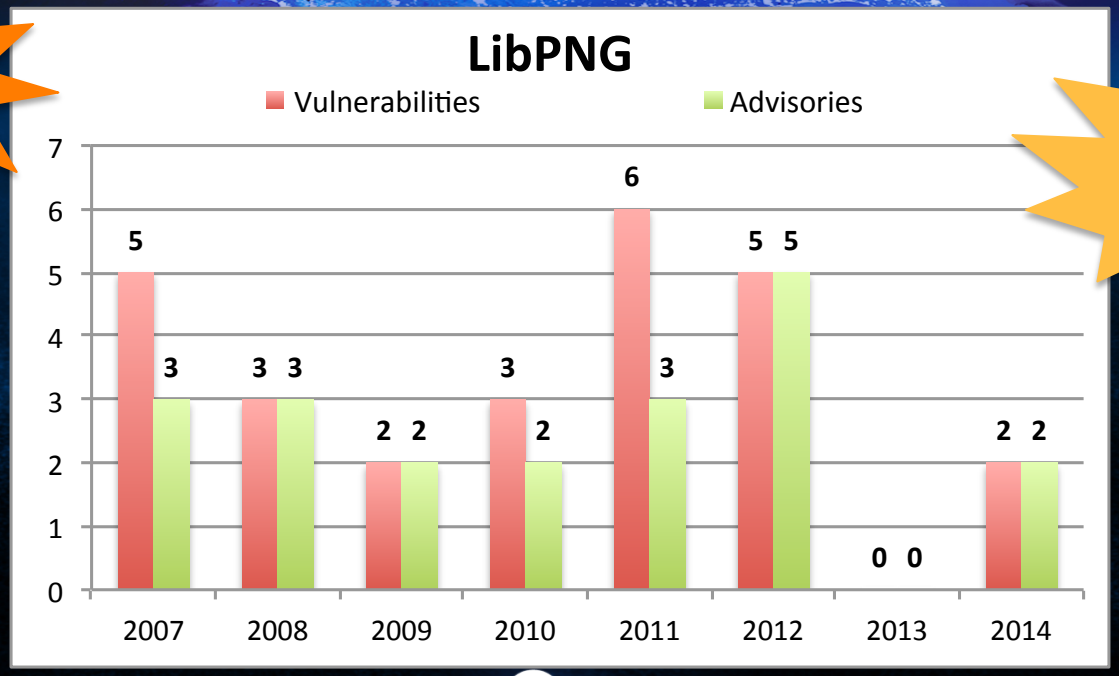
the FreeType Project

Vuln Spread:

And also… OSX, Webkit, Firefox, OpenJDK, OpenOffice, StarOffice, Ubuntu, Gentoo, Oracle Solaris, SUSE, Slackware, BlackBerry products, Fedora, RedHat, Debian, Avaya products, PlayStation 3/4/Vita, Opera for Wii, multiple video games…

libpng

26 Vulns



3 releases per year

Average CVSS 6.58

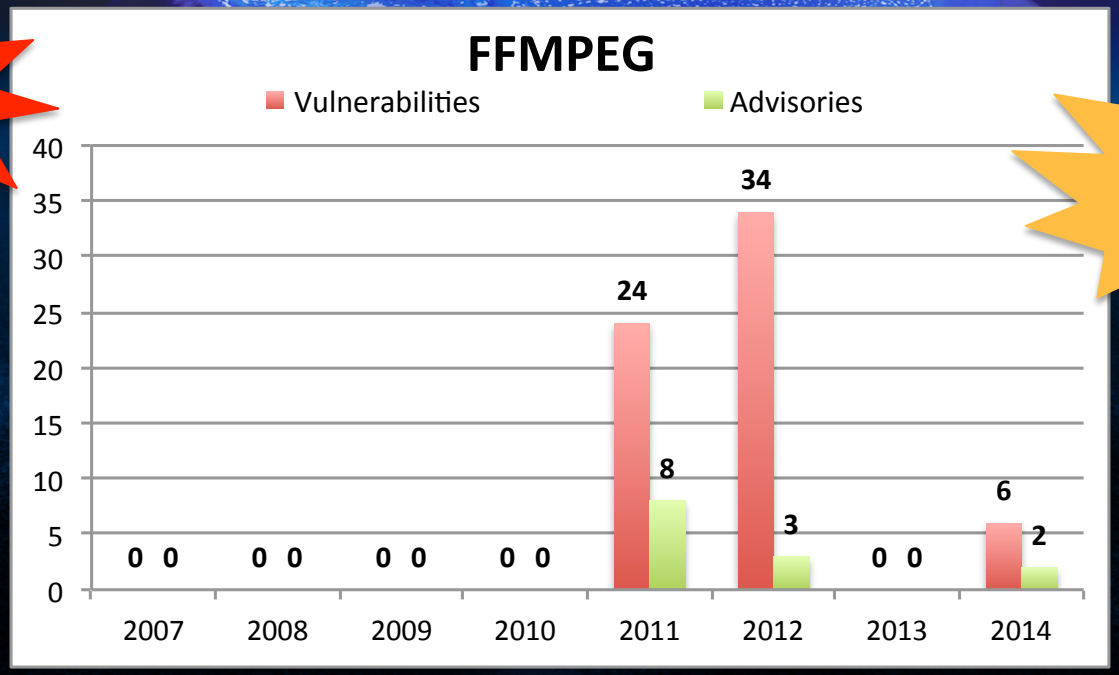
libpng

Vuln Spread:

Visio, PowerPoint, Adobe Photoshop/Flash/Illustrator, Webkit, iOS, OSX, Android, GIMP, Fedora, Debian, Ubuntu, Slackware, Red Hat, SUSE, Gentoo, Oracle Solaris, VMWare Server, and countless applications.

FFMPEG

64 Vulns



3 releases per year

Average CVSS 8.35

FFmpeg

Vuln Spread:

YouTube, Chromium, ChromeOS, QuickTime, JavaCV, DirectShow, DropCam, Gstreamer, Mplayer, xine, PlayStation, Gentoo, Ubuntu, Debian, FreeBSD, Mandriva Linux, LaunchPad, Libav..


black hat
USA 2014
WHAT'S BEING DONE CURRENTLY?


ACCOUNTABILITY

Code Quality

Everyone *could* look at it,
but they don't.
Accountability for quality is deferred.

Code Quality

Bad code is just that, bad code and exists in Closed Source as well.


SHOW
ME THE
MONEY!

Money That's What We Need!

- Many projects are not well funded or resourced
- Bug bounty programs
  - Crowd source more eye on critical software or websites
- Code audit initiatives
  - TrueCrypt
  - OpenSSL

Core Infrastructure Initiative first round funding, announced 29May14: Network Time Protocol, OpenSSH and OpenSSL.

OpenSSL will receive funds for two, fulltime core developers. The OpenSSL project is accepting additional donations, which can be coordinated directly with the OpenSSL Foundation (contact at info@opensslfoundation.com).

The Open Crypto Audit Project (OCAP) will also receive funding in order to conduct a security audit of the OpenSSL code base. Other projects are under consideration and will be funded as assessments are completed and budget allows.

Forking For Quality!

- Premise being that it is the only way to ensure the code is secure is to own responsibility for the code.
- Companies and groups are forking libraries
  - Google Blink (Webkit)
  - OpenBSD LibreSSL (OpenSSL)

threat post

CATEGORIES | FEATURED | PODCASTS | VIDEOS

07/16/14 8:27

Content Security Policy Mitigates #XSS, Breaks Websites - http://t.co/szwstL2cS2

Welcome > Blog Home > Cryptography > 'Overblown' LibreSSL PRNG Vulnerability Patched

"catastrophic failure"...

"unsafe for Linux"

'OVERBLOWN' LIBRESSL PRNG VULNERABILITY PATCHED

by Michael Mimoso Follow @mike_mimoso July 16, 2014 , 8:25

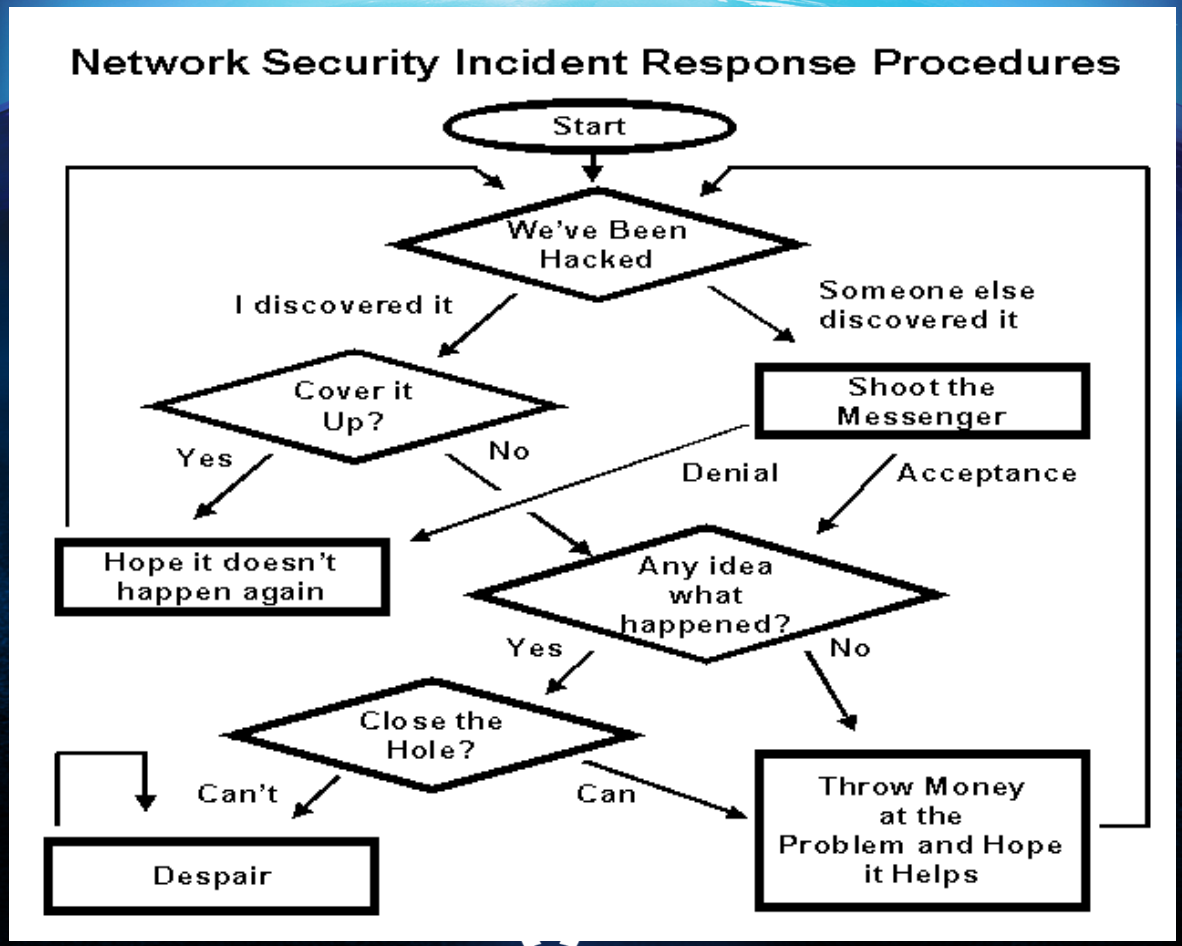
The OpenBSD project late last night rushed out a patch for a vulnerability in the LibreSSL pseudo random number generator (PRNG)


black hat
USA 2014
ACTIONS


RISKS
AHEAD

Know What You're Committing To

- Evaluate vuln trends in libraries as part of selection criteria
- Do you have enough people resources to handle the expected vulnerability load?
- What is your prioritization model?
- What early monitoring processes can you put in place to minimize surprises?
- Can you identify low friction areas to diminish risk?
- Communicate, communicate, communicate


Network Security Incident Response Procedures
Start
We've Been Hacked
I discovered it
Someone else discovered it
Cover it Up?
Shoot the Messenger
Yes
No
Denial
Acceptance
Hope it doesn't happen again
Any idea what happened?
Yes
No
Close the Hole?
Can't
Can
Throw Money at the Problem and Hope it Helps
Despair

Incident Response

1 Identify Issue → 2 Assess Impact → 3 Dev & Test Fix → 4 Public Release w/ CVE → 5 Post Release

But wait!
The vulnerability was in a third party library!

So you're a software vendor…

1 Identify Issue → 2 Assess Impact → 3 Dev & Test Fix → 4 Release → 5 Post Release

Enterprise admin?
Your patch lifecycle starts HERE

Vendors, Monitor Your Libraries!

- Source code scanning tools
- Vulnerability Database providers
- Your Legal Team is your friend

What Else Can Be Done? (dev edition)

- Vendor security testing
  - Active security testing of third party and OSS libraries using in house and/or outsourced security researchers
- Proactive plan for routine patching as part of dev lifecycle
- Robust Incident Response Plans for critical vulnerability disclosures that include Dev Team resources for product sustainment

What Else Can Be Done? (IT edition)

- Network scanning - know what software is in use where.
- Know where risk is in your environment
  - Monitor OSS advisory releases for software used in your apps/ products.
  - ASK your SW Vendors if they are affected by third party vulns
  - Code and Network scanning for un-patched vulnerabilities.
- Plot the vulnerability trends for your environment
- Plan time for sustainment


black hat
USA 2014
DISCUSSION!


black hat
USA 2014
EPIDEMIOLOGY OF SOFTWARE VULNERABILITIES: A STUDY OF ATTACK SURFACE SPREAD
Kymberlee Price
@Kym_Possible
Director of Strategic Operations
Synack
Jake Kouns
@jkouns
CISO
Risk Based Security