

at

ACQUIDA™

Marc Seeger (@rb2k)
Boston Devops Meetup
May 20th 2014

Act 1: Technology

How it all started

7:24 PM



Marc ★★★★★
@rb2k

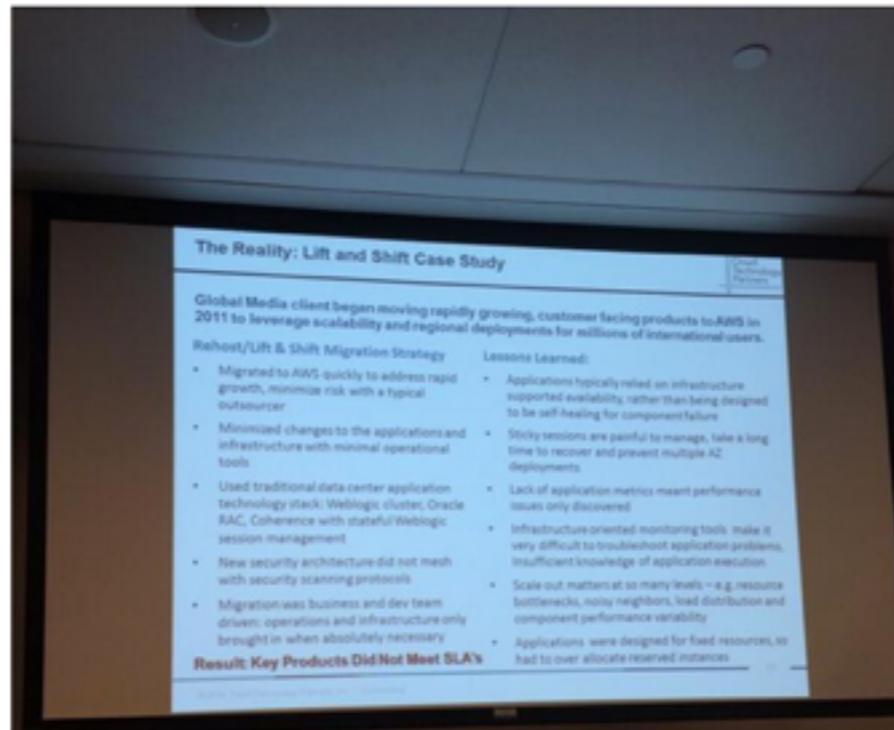
Meh, management presentation...

[#bulletpointgalore](#) pic.twitter.com/ttjJb4C3t

[View translation](#)

[from Cambridge, MA](#)

[Reply](#) [Delete](#) [Favorite](#) [More](#)



How it all started

7:30 PM

 [Marc](#) ★★★★★ @rb2k · Apr 7
IP, TCP, and HTTP - Syncing Data - objc.io issue #10 j.mp/1clubFR via
[@instapaper](#)
[Expand](#) [↩ Reply](#) [🗑 Delete](#) [★ Favorite](#) [⋮ More](#)

How it all started

7:26 PM



snipe
@snipeyhead

 [Following](#)

Info on the OpenSSL Heartbleed Bug
snipe.ly/1en58Dr

 Reply  Retweet  Favorite  More

RETWEETS	FAVORITES	
14	6	

7:26 PM - 7 Apr 2014

How it all started

7:33 PM

☆ **Marc Seeger** <marc.seeger@acquia.com>

To: hosting-eng Engineering
OpenSSL Heartbleed Bug

7 Apr 2014 19:33

[Hide Details](#)

Sent - acquia 1



<http://heartbleed.com/>

I'm on my phone at the moment, but that doesn't sound fun.

Sent from my iPhone

How it all started

 Retweeted by Marc ★★★★★

 **Melissa** △ @0xabad1dea · Apr 7
I no longer even have the capacity to be surprised by or upset with SSL. You could tell me it murders children and I would be like k

Expand ← Reply  Retweeted ★ Favorite ⋮ More

 **Marc** ★★★★★ @rb2k · Apr 7
Ugh, another OpenSSL bug. This one is bad: heartbleed.com

Update your stuff.
Now.

Expand ← Reply  Delete ★ Favorite ⋮ More

Quick risk assessment

Lucid:

```
[00:35:27] root@bal-2.dev:~# openssl version  
OpenSSL 0.9.8k 25 Mar 2009
```

Precise:

```
[00:34:37] root@master.dev:~# openssl version  
OpenSSL 1.0.1 14 Mar 2012
```

Where's ~~Waldo~~ OpenSSL



8000 EC2 Machines:

- 99.9% of them puppetized
- Candidates:
 - Balancers
 - SVN Servers
 - Appliances
 - ELBs
 - 3rd party AMIs
 - Unique little snowflakes (Jira, Crucible,...)

Let the patching begin

CL-1 | Chatroom: Update the nginx build script to a non-vulnerable ve... [Browse code](#)

...rsion of openssl.

🔒 master 🔗 1.77.8 ... 1.77.0

 rb2k authored on Apr 7 1 parent [604275a](#) commit [d52b709aa7ee6ab6da402d554f44c13979fb976b](#)

📄 Showing 1 changed file with 2 additions and 2 deletions. [Show diff stats](#)

4  tools/build/build_scripts/nginx.sh [View](#)

Line	Old	New	Code
			@@ -13,9 +13,9 @@ OS=\$(lsb_release -cs)
13	13		BASEDIR=\$(pwd)
14	14		
15	15		NGINX_VERSION="1.4.4"
16		16	-BUILD_VERSION="1" # Increase for modifications in the packaging. Reset to 1 when the nginx version changes.
		16	+BUILD_VERSION="2" # Increase for modifications in the packaging. Reset to 1 when the nginx version changes.
17	17		# Since lucid has a <1.0.1 OpenSSL, we add the latest to support TLSv1.[12], FS,...
18		18	-OPENSSL_VERSION="1.0.1e"
		18	+OPENSSL_VERSION="1.0.1g"
19	19		# Pagespeed is disabled due to https://github.com/pagespeed/nginx_pagespeed/issues/492
20	20		PAGESPEED=0 # 0 to disable including pagespeed in the build
21	21		

Rollout



Australia:

Con:

- Spiders
- Snakes

Pro:

- Ops is awake

Rollout



Scan



Waiting on ELBs...



Internal Certificates

REGENERATE



Suddenly:
“reverse” Heartbleed



Act 2: Communication

Internal

- Pre-determined chat rooms
- Dial-in conference bridges
- A communication plan



Thanks SSAE-16, PCI and FedRAMP... I guess :)

Statuspage + Twitter

*

Heartbleed vulnerability 2014-04-07

Incident Report for Acquia, Inc.

Resolved

We have completed the unscheduled maintenance to update the Acquia Cloud platform against the Heartbleed vulnerability.

IMPORTANT: Affecting Acquia Cloud Sites. Please take additional action to secure your site. Please visit <https://docs.acquia.com/heartbleed> for more information.

Posted about 1 month ago

Monitoring

We are continuing to monitor Acquia Cloud customer sites for any signs of the vulnerability at this time. For more information on the vulnerability, including how to secure your site, please visit <https://docs.acquia.com/heartbleed>.

Posted about 1 month ago

Identified

We are aware of a recently announced security issue with the OpenSSL cryptographic library. We have initiated maintenance to ensure our sites are protected against the vulnerability.

Posted about 1 month ago. Apr 08, 2014 - 4:00AM UTC



Acquia Support

@acquia_support



Following

We are aware of a recently announced security issue with the OpenSSL cryptographic library. Please visit status.acquia.com for info.

Reply Retweet Favorite More

RETWEET

1



12:15 AM - 8 Apr 2014

Documentation

<https://docs.acquia.com/articles/heartbleed-acquia-cloud>

Heartbleed (CVE-2014-0160) on Acquia Cloud

On April 7, 2014, a security vulnerability with servers running the OpenSSL cryptographic library was revealed at <http://heartbleed.com>. The security advisory for this vulnerability is [CVE-2014-0160](#). Acquia has completed maintenance on all servers and infrastructure to close this vulnerability and ensure that Acquia Cloud customer sites are protected.

For more information on Acquia's response to Heartbleed, please see the blog post [Protecting Enterprise Drupal Users Against Heartbleed](#).

Actions to take

At this time Acquia is recommending that customers should complete the following actions:

1. [Rekey](#) your SSL certificates. Customers should read the first FAQ question in the next section to determine the action they need to take for their sites and begin the process to retrieve their rekeyed certificate from their Certificate Signing Authority (CSA), if necessary.
2. Reset your Drupal passwords, especially site administrative password(s) and the passwords of any users with elevated permissions. See the following document for further information: [How do I reset my admin password in Drupal 7?](#)
3. Audit all SSH keys. See [Adding a public key to your server](#) for information on viewing your keys.
4. Reset all Acquia Network passwords.

FAQ

Here are the answers to some common questions:

How can I tell if I am affected?

- If you are not using SSL on your website, you are not affected by this security vulnerability, and you can ignore this article.
- If you are using SSL on your website, you are affected and you should rekey your SSL certificate as

Proactive communication



Phone calls by Acquia support, TAMs, ...

Since then: Post mortem



Since then: Incident Commander



(shamelessly stolen from Heroku)

http://en.wikipedia.org/wiki/Incident_command_system

Since then:

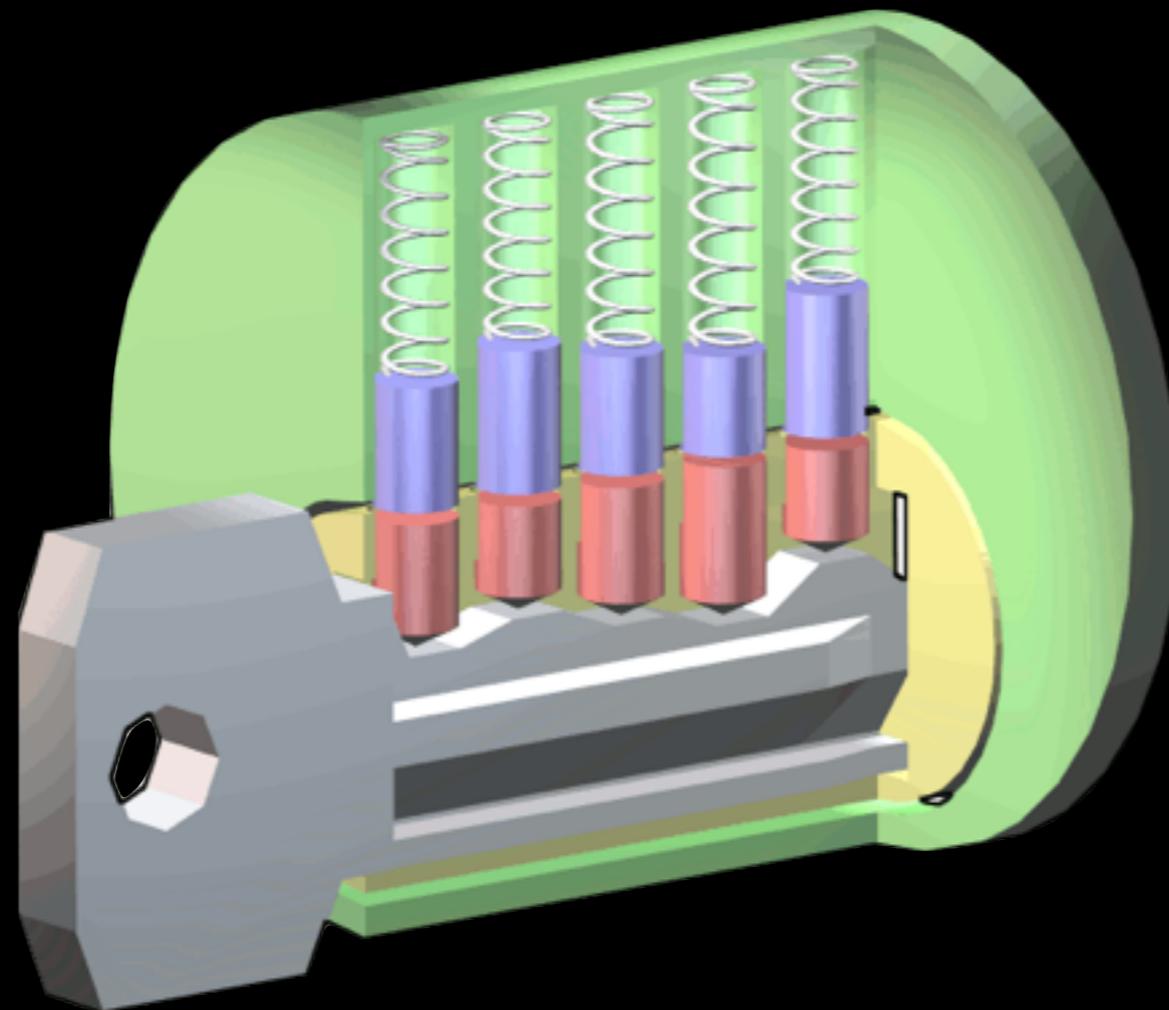
Dedicated resource to vet security threats

**IF YOU SEE
SOMETHING,
SAY
SOMETHING.**

Since then: Clean up intranet docs



Since then:
Additional tooling



We're hiring

(shameless self promotion)

bit.ly/acquiaajobs

Engineering

[Cloud Software Engineer](#)

Burlington, MA United States

[Cloud Systems Engineer](#)

Burlington, MA United States

[Cloud Systems Engineer \(EMEA\)](#)

Reading, United Kingdom

[Director, Platform Tools & Services](#)

Burlington, MA United States

[Distributed Systems Cloud Engineer](#)

Burlington, MA United States

[Drupal Engineer](#)

Burlington, MA United States

[Senior Cloud Systems Engineer](#)

Burlington, MA United States