Advanced Vulnerability Management in Cloud Foundry

Molly Crowther
Senior Technical Program Manager &
member of CFF Security Team

Stephen Levine
Staff Software Engineer &
CF Buildpacks Project Lead

Pivotal
Pivotal
What we’re going to talk about

- CF as a secure platform
- Process - before + after
- DAVOS workflow
- How you can help
Team Kudos

• Thank you to everyone who has worked on Triage / Automation so far!
• Rasheed Abdul-Aziz, Julien Cherry, Anthony Emengo, Zamir Johl, Mike Kent, Neha Kumari, Simon Kwok, Harlie Levine, Ben Moss, Anne Thomas, Anna Thornton, and Matt Zinicola
Before we get too far...

- DAVOS - not just the guy from Game of Thrones + a town in Switzerland
What is DAVOS?

• “Dependency And Vulnerability Overlord System”
• DAVOS for short
• Built by Pivotal Security Automation Team
• Collects and stores data about vulnerabilities and integrates with Tracker to alert OSS and PCF teams + collect information from them
• We think this is kind of a new thing
Why?
Heartbleed

• Disclosed in 2014, in OpenSSL since 2012

• “Some might argue that Heartbleed is the worst vulnerability found (at least in terms of its potential impact) since commercial traffic began to flow on the Internet.” - Joseph Steinberg in Forbes

• Ubuntu stemcells not affected but CentOS were

• Before CF had a process in place for disclosing vulnerabilities
Dirtycow

- Went public on October 19, 2016
- Linus Torvalds committed the fix + said that he had tried to fix it 11 years prior
- One of the first CVEs to get a Live Patch from Canonical
- All stemcells affected
- New Ubuntu stemcells released October 20
- Logos, wiki, website, t-shirts?
Case Study:
Ubuntu Security Notices
What it looks like in theory...
OSS upstream patches
OSS upstream patches

Canonical patches Ubuntu
OSS upstream patches

Canonical patches Ubuntu

CF patches rootfs

CF patches stemcell
OSS upstream patches

Canonical patches Ubuntu

CF patches rootfs

Runtime patches

Public Notification

CF patches stemcell
OSS upstream patches

Canonical patches Ubuntu

CF patches rootfs

Runtime patches

Public Notification

CF patches stemcell

Other services patch
OSS upstream patches

Canonical patches Ubuntu

CF patches rootfs

Runtime patches

Public Notification

CF patches stemcell

Other services patch
So what’s the problem?

- Surprise! High USNs need to be patched faster.
- Public notification is hard
and...
What it really looks like...
Ubuntu Security Notices
Ubuntu Security Notices

Github Issues
Ubuntu Security Notices

Github Issues

Ubuntu Website

USN-3428-1: Emacs vulnerability

Ubuntu Security Notice USN-3428-1

class_ascensor

emu247vulnerability
Ubuntu Security Notices

Github Issues

Slack

Ubuntu Website

CLOUD FOUNDRY SUMMIT 2017
BOSH Stemcell Scraper

Black box?

Trackers

Cloud Foundry

CLOUD FOUNDRY

CVB-2017-0048: Cloud Controller API regression
by Cloud Foundry Foundation Security Team  |  Published 29th November 2017

cloudfoundry.org
Patching the RootFS: USN to production in ~2 hours ...but only if you're paying attention
RootFS Patch Process

When a USN hits, the CF Buildpacks pipeline automatically releases a new RootFS in < 2 hours.
RootFS Patch Process

Cloud Foundry allows operators to patch the OS-level dependencies of every app in their deployment with a single `bosh deploy`! Unlike container image layer based platforms...

Talk about CF taking advantage of ABI compatibility vs. Docker/Rocket
RootFS Patch Process

But not every USN is relevant to apps running in the platform.

Ubuntu Security Notice USN-3246-1

27th March, 2017

Software description

- eject - ejects CDs and operates CD-Changers under Linux
Patching the Stemcells:
Kernels make everything terrible...
Stemcell Patch Process - Differences from RootFS

- High kernel CVEs are common
- RootFS ➔ one platform, Stemcells ➔ many platforms
- Need VMs to build stemcells
- Other things the BOSH team knows about
How do Cloud Foundry vendors, teams, and operators know when to patch their RootFS and Stemcell?
How do Cloud Foundry vendors, teams, and operators know when to patch their RootFS and Stemcell?

Or really any BOSH release?
So what does DAVOS do?
High-level overview

Sources of Data
High-level overview

Sources of Data

USNs

New versions of golang, NGINX, etc.
High-level overview

Sources of Data

- USNs
- New versions of golang, NGINX, etc.
- General notices
High-level overview

Sources of Data

- USNs
- New versions of golang, NGINX, etc.
- General notices

DAVOS
High-level overview

Sources of Data

- USNs
- New versions of golang, NGINX, etc.
- General notices

DAVOS

Tracker

- Tracker A
- Tracker B
- Tracker C

Tracker C
High-level overview

Sources of Data

USNs

New versions of golang, NGINX, etc.

General notices

DAVOS

Tracker

Tracker A

Tracker B

Tracker C

Tracker C
High-level overview

Sources of Data
- USNs
- New versions of golang, NGINX, etc.
- General notices

DAVOS
- Notices

Tracker
- Tracker A
- Tracker B
- Tracker C
- Tracker C
High-level overview

Sources of Data
- USNs
- New versions of golang, NGINX, etc.
- General notices

DAVOS
- Notices

Tracker
- Tracker A
- Tracker B
- Tracker C
High-level overview

Sources of Data
- USNs
- New versions of golang, NGINX, etc.
- General notices

DAVOS
- Product A
- Product B
- Product C

Tracker
- Tracker A
- Tracker B
- Tracker C

General notices
What’s next? How can you help

• Bringing DAVOS to the ecosystem by suggesting for incubation

• Generalizing so deployment is possible for other foundation members

• Suggestions and feedback welcome to mcrowther@pivotal.io or @mcrowther in OSS slack
Thanks for coming!

Questions?