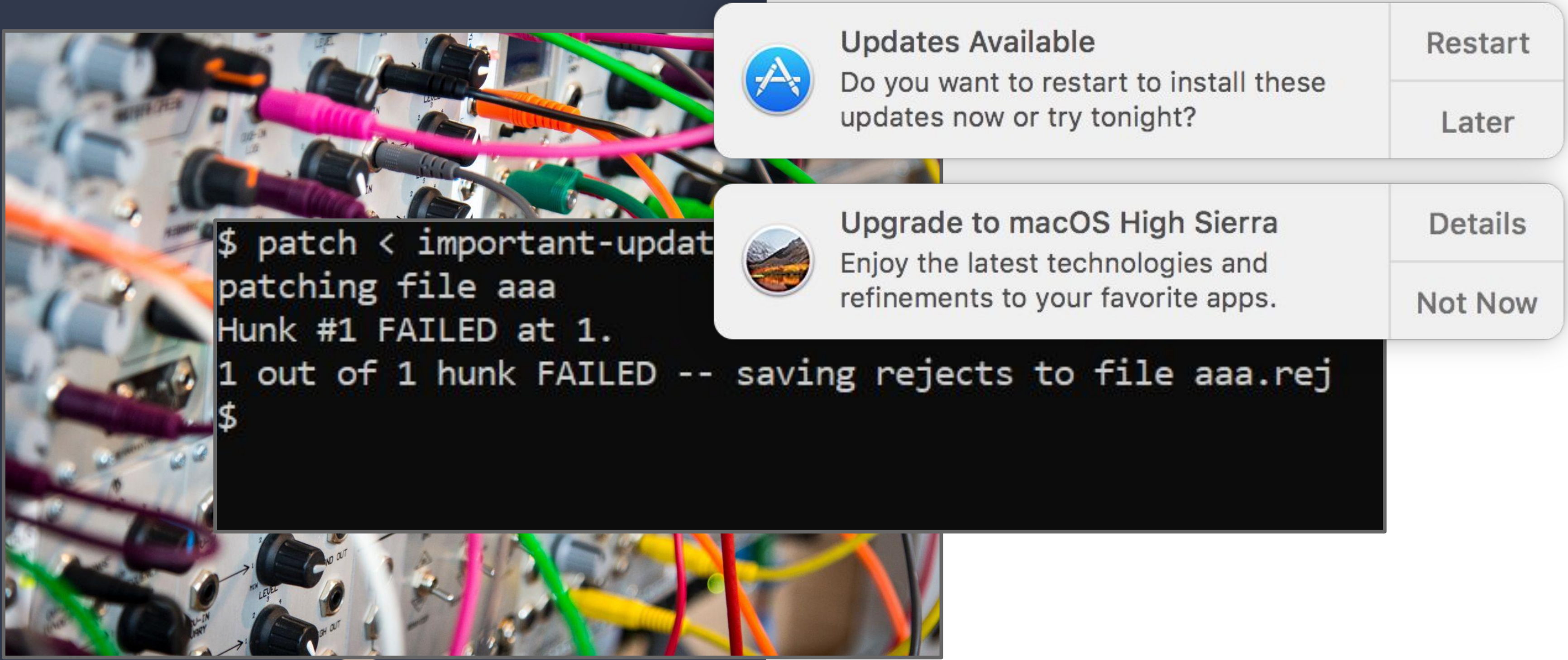
Software patching needn't be a can of worms

SREcon EMEA 2019
Philip Rowlands



```
$ patch < important-updat
patching file aaa
Hunk #1 FAILED at 1.
1 out of 1 hunk FAILED -- saving rejects to file aaa.rej
$
```

Updates Available

Do you want to restart to install these updates now or try tonight?

Upgrade to macOS High Sierra

Enjoy the latest technologies and refinements to your favorite apps.

Photo by John Barkiple on Unsplash

import std_disclaimer

- Opinions are mine
- Trademarks are theirs
- Copyrights are inline
- Zero warranty express or implied
- Void where prohibited

Intro

> *"There's no record of what third-party software or versions we use. I don't know what updates are available, and of those, which are the most important. It's hard to get downtime on production systems. There's no test environment for this. I'm scared the upgrade will break stuff, and when it does, rolling back will be even harder."*
>
> *-- You, possibly*

If this is the problem, automation is the solution.

Vendor Approaches

Real Life example #1 fully automated

- Phones - iOS, Android
- Operating Systems - macOS, Windows
- Smart TVs
- Web browsers

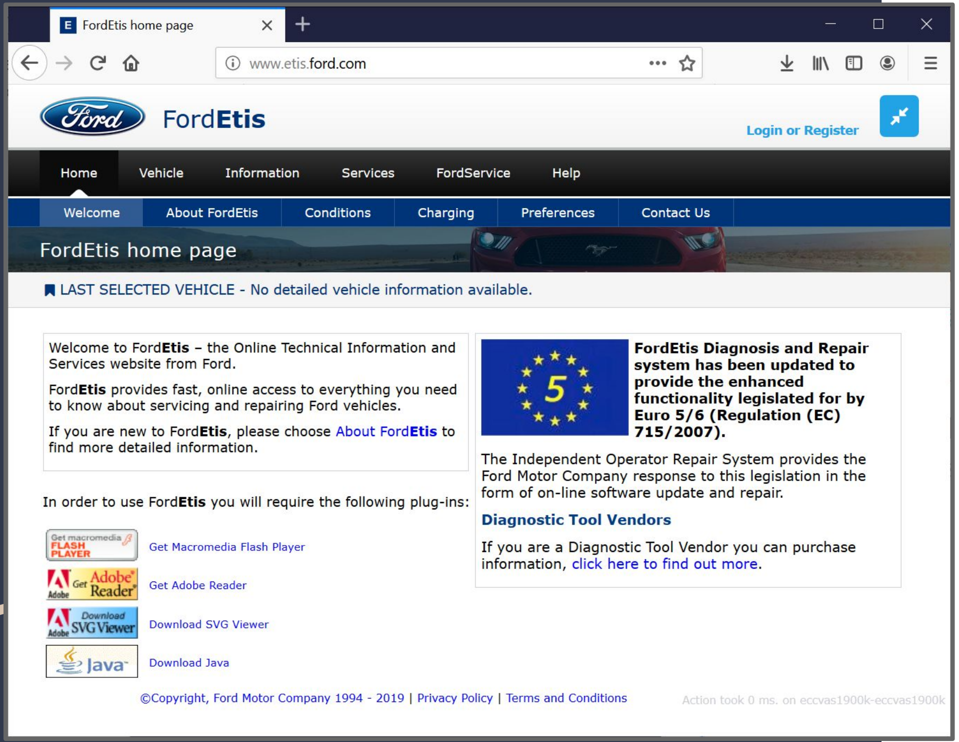
Real Life example #2 semi automated

- Linux package managers e.g. DNF, APT
- VOIP phones
- Either the software has its own freshness-check feature, or sidecar tools to compare versions and deliver updates
- Any software that can check its own status (not just a URL)

Real Life example #3 - fully manual

- No help from software or package management
- You do all the legwork to discover and bring in new versions
- e.g. tar files downloaded directly / built from source
- e.g. COTS software with no version awareness

Case study: Cars



FordEtis home page

LAST SELECTED VEHICLE - No detailed vehicle information available.

Welcome to Ford**Etis** – the Online Technical Information and Services website from Ford.

Ford**Etis** provides fast, online access to everything you need to know about servicing and repairing Ford vehicles.

If you are new to Ford**Etis**, please choose About Ford**Etis** to find more detailed information.

In order to use Ford**Etis** you will require the following plug-ins:

FordEtis Diagnosis and Repair system has been updated to provide the enhanced functionality legislated for by Euro 5/6 (Regulation (EC) 715/2007).

The Independent Operator Repair System provides the Ford Motor Company response to this legislation in the form of on-line software update and repair.

Diagnostic Tool Vendors

If you are a Diagnostic Tool Vendor you can purchase information, click here to find out more.

©Copyright, Ford Motor Company 1994 - 2019 | Privacy Policy | Terms and Conditions

Action took 0 ms. on eccvas1900k-eccvas1900k

- All major manufacturers run "Technical" websites providing paywall access to software for cars
- e.g. Ford **Etis**, VW **erWin**
- Tesla - Over The Air updates
- Caution: Chrysler UConnect

Single update track vs LTSB

Does the vendor distinguish security / bugfix / feature releases?

For example, Firefox Extended Support Release, Linux LTS, Windows 10 LTSC, Cisco NX-OS Long Lived release.

For example, Red Hat Enterprise Linux Maintenance Support Phase, or Solaris 10 Extended Support (until Jan 2021).

Automation To The Rescue

Overview

- Inventory
- Awareness
- Assessment
- Planning / Risk
- Rollout / Rollback
- GOTO 10

Automation: Inventory

- ❖ Awareness
- ❖ Assessment
- ❖ Planning / Risks
- ❖ Rollout / Rollback

- The goal is to draw together all the data about what third-party software you’re running
- Enterprise vendors may provide tooling for this, e.g. Dell OpenManage
- Roll your own, but check first for existing tools
- Coverage - is everything network-accessible?
- Zombies - is everything network-accessible right now?

Automation:

- Inventory

Awareness

- Assessment
- Planning / Risks
- Rollout / Rollback

- Now you know what's running, what updates are available?
- e.g. ~~MSBA~~ Windows Update offline scan file, yum repos, Solaris patchdiag.xref

Automation:

- Inventory
- Awareness

Assessment

- Planning / Risks
- Rollout / Rollback

- Should we take every update / release?
- Classify into now, soon, sometime / never
- In-house assessment vs delegation to vendor / distro / third-party (Snyk)
- Safer to assume that every version you run will sooner or later be replaced with a critical security update.

Automation:

- Inventory
- Awareness
- Assessment

Planning

- Rollout / Rollback

When to apply? Is downtime required? If so, do we have a maintenance window? If not, when?

What level of redundancy?

N+0	2AM Sunday
N+1	Tolerate single failure
N+2	Tolerate single failure + maintenance

If horizontal scaling, can you apply a rolling update, or is a flag day needed?

Automation:

- Inventory
- Awareness
- Assessment

Risks

- Rollout / Rollback

Proactive risks include:

- fat-finger error,
- startup bitrot,
- introducing new bugs / regressions

Reactive risks include:

- major version jump
- EOL version no longer supported
- unfamiliar work
- 20-step manual process
- ignores “many eyes”

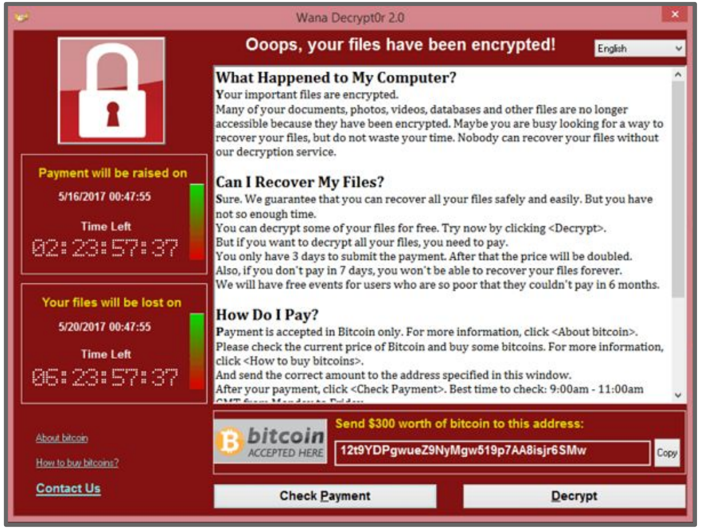
Case study: WannaCry vs NHS

"The majority of NHS devices infected were running the supported, but unpatched, Microsoft Windows 7 operating system. Unsupported devices (those on XP) were … decreased … to 1.8 per cent in January 2018."

-- NHS Improvement postmortem

Timeline:

- 2009-04-14 Windows XP support ends
- 2017-03-14 MS17-010 update published to disable SMBv1, "**Critical** - Remote Code Execution"
- 2017-05-12 Ransomware worm
- 2018-02-01 Postmortem published



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Automation:

- ❖ Inventory
- ❖ Awareness
- ❖ Assessment
- ❖ Planning / Risks

Rollout / Rollback

Easier to justify rollout for a new version if rollback is available and simple.

Is there a test for the intended change? If not, we must rely on regression, stability and performance.

The new version must not fail any tests we run, nor crash, nor exhibit (more) errors, nor use +%50 CPU.

For example, full mitigations for Meltdown & Spectre issues reduced CPU performance by Intel's own benchmarks.

Gain confidence with comprehensive QA automation (CI), and/or incremental rollout (5%, 15%, 50%, 100%)

then do it all over again

Assertion: there is no bug-free software

Corollary: eventually all maintained software will have an available update

Trigger Warning: Update Available

Don’t stop at Security

If you have a Security team, they probably already do some of this, at least for the vulnerabilities which have names (Dirty COW, Spectre, Meltdown, Heartbleed, Shellshock, POODLE, DROWN).

Why not task the folks already doing this work to go beyond security fixes when considering Inventory, Awareness, Assessment etc.?

Everything dies

Some commercial software gives several years' notice; some OSS project may simply stop updating, or lose a maintainer.

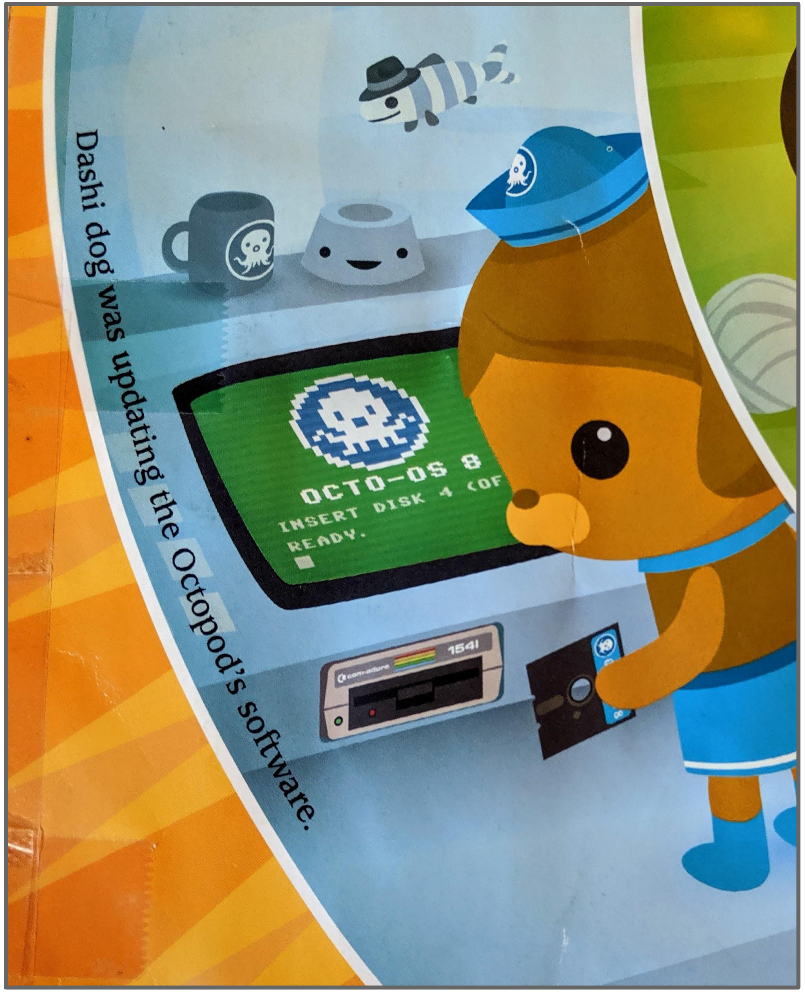
IBM's VM/370 (1972), still updated as z/VM in 2018.

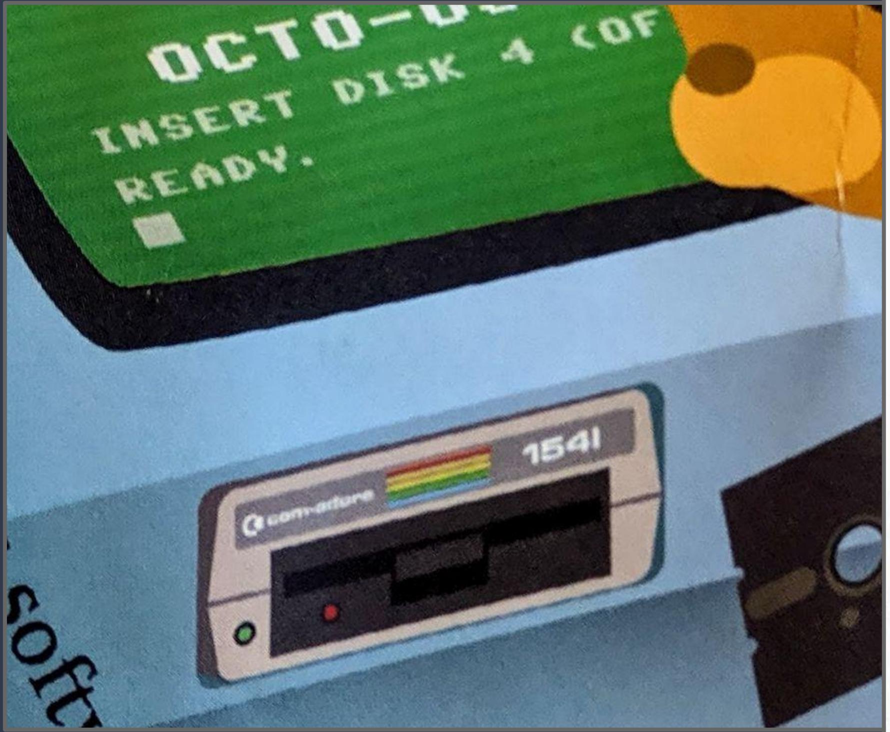
Do you know your third-party software's end-of-life? Is there an available major upgrade? It might take months to migrate and deploy. e.g. Windows 10 desktops.

Caution: not easily automatable

Case study: The Octonauts Explore the Great Big Ocean

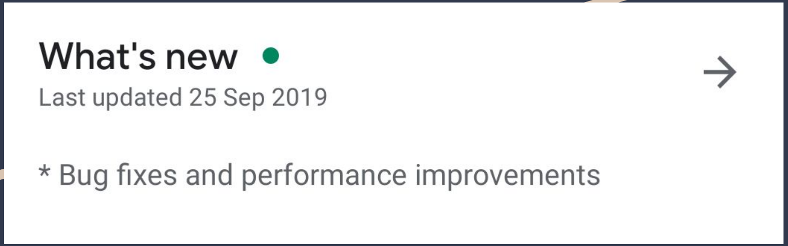
“Dashi dog was updating the Octopod’s software”




OCTO-
INSERT DISK 4 (OF
READY.
commodore
1541
soft

commodore
1541

Bug fixes and performance improvements



What's new ●

Last updated 25 Sep 2019

* Bug fixes and performance improvements

Release notes are mostly useless. Do you have time to read them?

Helpful if release notes tell you:

- CVE issues resolved
- Vendor/distro urgency (Critical, Important, Optional)

If risk averse, it’s reasonable not to apply updates under 1 month old, and let others find the regressions.

Incremental automation

What do you already have which could be built upon?

- ❖ Inventory
- ❖ CI / CD
- ❖ Release engineering

The 2nd best day to start is today

You're more likely in the situation where things are in a poor state, rather than greenfield patching planning.

As retro-fit work, benefits are realised incrementally.

Virtuous side-effects of automation as applied to your in-house software.

Further reading

Stuff that didn’t fit in the small margin of this talk:

- Linux Vendor Firmware Service
- Container Image Security scans
- Huawei OpenSSL proliferation

That's All Folks

- What can we automate?
- What can we delegate?
- Which incidents would have been avoided?