Building a Better Patching Plan: VAC's Patch Management Strategy

May 2021

In the Beginning!

In fiscal year 2014-2015:

VAC had over 287 infections registered across our desktop environment

We patched… when we could…

We were busy fighting fires!

We ran… a pretty standard patching business

……Pretty Risky!

So what did we do?

We got serious about patching:

We put in a processes

We put in the tools

We put in standards

We set expectations

Let's Get Technical!

- Today, Veterans Affairs Canada applies desktop patching and monitoring on four separate technical platforms.

Physical Windows 10

Laptops and Desktops with a local Windows 10 installation, in the following locations:

- Charlottetown Head Office
- Ottawa Head Office
- Laptop presences in Area Offices

Legacy Wyse (ThinOS) terminals

In addition to laptops, all offices which connect to VDI have ThinOS terminals which solely present users with a VDI session. Patches to these devices are not released as frequently, thus reviewed on a semi-annual basis.

Virtual Desktop Infrastructure (Legacy VDI)

All other VAC offices, including European Operations in France, connect to virtual desktops, which are housed in the Moncton Data Centre. VDI enables our VAC users to connect to their personalized desktop from virtually any VAC computer or location, as well as connectivity for external partners such as the Royal Canadian Legion and Department of Justice.

Apple devices

VAC currently has 10-12 Macbooks connected to the VAC network, which are currently patched manually. A centralized management solution is currently under investigation.

What content is VAC IT patching?

Operating Systems

- Microsoft Windows 10
- VDI & Physical Windows 10
- Wyse ThinOS Terminals

Web Browsers

- Internet Explorer & Edge
- Google Chrome
- Mozilla Firefox

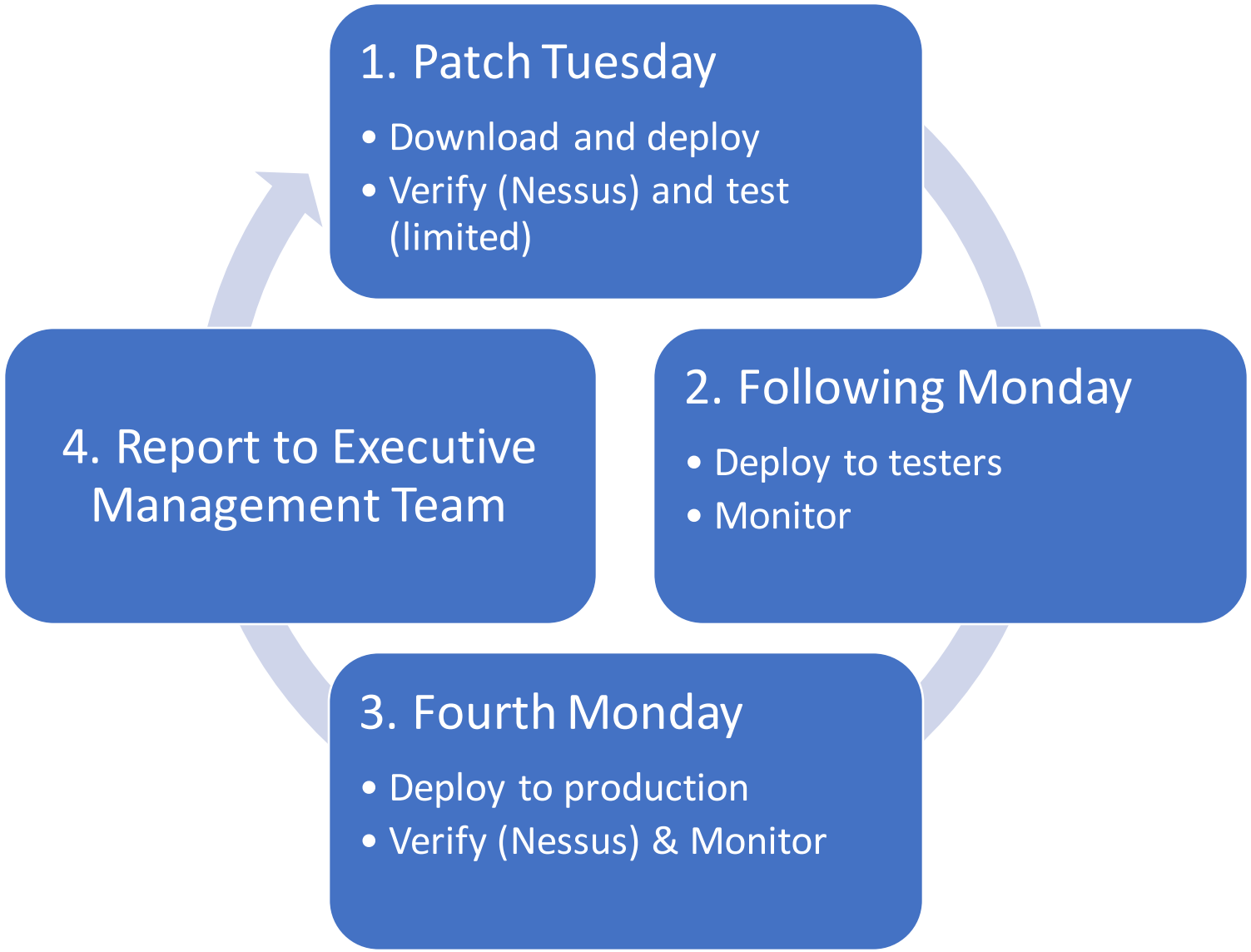
Plug-ins

- Java
- Adobe Flash
- Adobe Reader

*Physical applications on Windows 10 are managed through Microsoft SCCM, and on VDI, are installed directly on our image.
**Virtual Applications delivered to all environments are distributed with Microsoft App-V

Patching Cycle!

- They key to good patching is consistency which helps manage expectation



Monthly Cycle

- Updates viewed as a package
  - Operating System
  - Java
  - Internet Explorer
  - Edge
  - Firefox
  - Chrome
  - Adobe Flash
  - Adobe Reader

VDI & Windows 10 Patch Testing Strategy

Phase One

Duration: 2nd Tuesday of the month – the following Monday

Phase One -> Patch Initial Testing:

- Second Tuesday of the month "Patch Tuesday", VAC's Desktop Engineering team downloads standard monthly patches (Windows Operating System, Web Browser & Plug-in) and prepares for installation.
- Once installed in the test environment, the IT Security team runs the Nessus scan utility to ensure there are no outstanding vulnerabilities in our environment that require patching. Patch content is updated as required.
- The following day (Wednesday), patches are deployed to a small subset of IT staff.
- Testing continues until Monday of the following week.
- Issues concerning patches are fielded directly by the Desktop Engineering team.

VDI & Windows 10 Patch Testing Strategy

Phase Two

Duration: 3rd Tuesday of the month – the following Monday

Phase Two -> Wider Patch Testing:

Following successful testing of Phase one, Phase Two Patch Testing begins:

- Third Tuesday of the month, patches are deployed to our testers across the country.
  - This testing team is comprised of key members of our Internal Business Application Development, a variety of typical user base across the Department, & all members of the National IT Service Desk
- Issues resulting from patches are reported to the National IT Service Desk.

VDI & Windows 10 Patch Production Deployment

Phase Three

Duration: 4th Monday of the month + install time

Phase Three -> Release:

- Pending a successful testing period, on the fourth Monday of the month, VAC National IT Service Desk communicates to all users to inform them that patches will be applied that evening, and advises all users to save their work & log off at the end of their work day.
- Physical Windows 10: Patches are installed throughout the day and applicable reboots occur during the maintenance window (23:00-06:00).
- VDI: The newly patched image is promoted for Production use after business hours and users who remain connected to their session are logged off ensuring that all are working in a patched state the following day.

Patch Issue Remediation

In the unlikely event that issues are discovered in Production, users are directed to contact our National IT Service Desk.

- Priority investigation occurs in collaboration with VAC's IT Security & Desktop Engineering teams.
- If the issues reported are as a result of deployed patches and a rollback is necessary, affected patches are retracted from our Physical Windows environment.
- In parallel, our VDI environment is updated and users simply log off and log back on to resolve any issues caused by the patching issue.

Reporting and Monitoring

Phase Four

Duration: First Tuesday of the month

Phase Four -> Report:

- After patches are deployed to production, IT Security once again runs the Nessus utility, and reporting information is provided to the IT executive management table, including outstanding patches that were rolled back, or had been released since patching was applied. The report lists the detail, including the criticality level for the vulnerability.
- IT Security performs regular reporting in special circumstances, such as patches that may have been rolled back during the patch cycle.
- Though we consider the process for VAC's patch cycle quite successful, thanks to the positive collaboration between our IT Security, Applications & Desktop Engineering teams, it remains under constant process improvement as new challenges are presented.

There's got to be exceptions…

- The key is to be flexible, agile and adapt

The need to be flexible

Critical Patches:

- In the event of a critical patch to high priority items such as zero-day vulnerabilities, we **"apply first, and ask questions later"**

Patching is not the only thing we do:

- We apply a multi-pronged approach, where patching is just one facet of our program (Phishing education and testing, etc.)
- We patch servers in a similar fashion with our SSC partners

We keep our partnerships engaged:

- We have a very good relationship with our key infrastructure partners (SSC)

So… How did it go?

The results are clear!

Virus Detection and Protection Services

Virus/Malware Infected Computers (Logged by IT SEC): An infected host with the intent to damage or steal information. IT Security routinely looks for these anomalies, determines their origin and completes the necessary steps to mitigate the risk to VA systems.

	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-21
YTD Total:	287	150	48	93	39	12	19

Reference: Veterans Affairs Canada - Quarterly Security Report

Teams are used to it, know what to expect, and it's just normal!