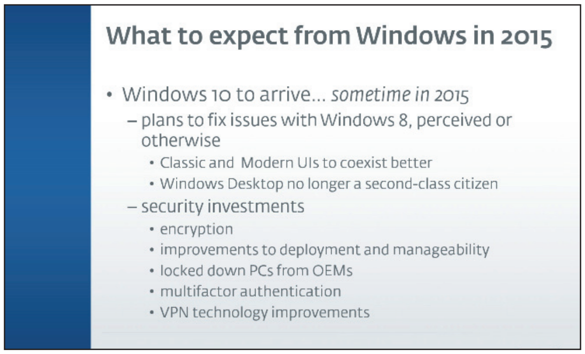
virus BULLETIN Covering the global threat landscape

# WINDOWS 10 PATCHING PROCESS MAY LEAVE ENTERPRISES VULNERABLE TO ZERO-DAY ATTACKS

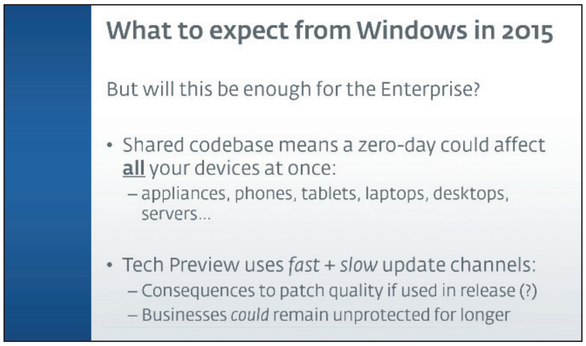
*Aryeh Goretsky*
ESET, USA

Last year, *ESET* presented a webinar [1] in which we discussed some of the improvements *Windows 10* is bringing to *Microsoft*'s flagship operating system. At the time of the presentation, not much had been publicly revealed by *Microsoft* about how the new operating system would be patched, although we did note that *Microsoft*'s use of fast and slow release channels for updates could mean that some users might be subject to buggy updates, while others could be exploited by zero-day [2] vulnerabilities:



What to expect from Windows in 2015

- Windows 10 to arrive… *sometime* in 2015
  - plans to fix issues with Windows 8, perceived or otherwise
    - Classic and Modern UIs to coexist better
    - Windows Desktop no longer a second-class citizen
  - security investments
    - encryption
    - improvements to deployment and manageability
    - locked down PCs from OEMs
    - multifactor authentication
    - VPN technology improvements



What to expect from Windows in 2015

But will this be enough for the Enterprise?

- Shared codebase means a zero-day could affect **all** your devices at once:
  - appliances, phones, tablets, laptops, desktops, servers…
- Tech Preview uses *fast* + *slow* update channels:
  - Consequences to patch quality if used in release (?)
  - Businesses *could* remain unprotected for longer

## WINDOWS UPDATES RELOADED

On 30 January, *Microsoft* published a new article in its Windows For Your Business blog, aptly titled 'Windows 10 for Enterprise: More secure and up to date' [3]. In the article, *Microsoft* explained its new patch roll-out strategy, which I will attempt to paraphrase below:

- A new Long Term Servicing (LTS) branch for businesses to use on mission-critical systems will deliver security and critical updates, but no new features. This sounds similar to the LTS [4] plans currently used by *Ubuntu* [5] and the *Mozilla Foundation* [6]. One major apparent difference is that *Windows 10* will have a much longer support cycle of ten years. This will comprise five years of mainstream support, followed by five years of extended support, as compared to *Ubuntu*'s five-year support and *Mozilla*'s one-year support model for their respective LTS branches.
- A current branch for businesses will provide security updates on a regular basis. Feature updates will be deployed as well, but on a less frequent basis in order to allow businesses to plan for them.
- Finally, consumers and *Windows Insiders* (*Microsoft*'s public beta test program) will receive all updates first – not just security and critical updates, but also new features and non-critical updates. Any bugs or crashes they come across in those updates will, presumably, be fixed before the updates are offered to enterprise users.

While splitting *Windows* users into different groups in order to test patches makes sense, and is something that many companies already do internally as a means of testing patches before a global roll-out, there are some downsides to this approach:

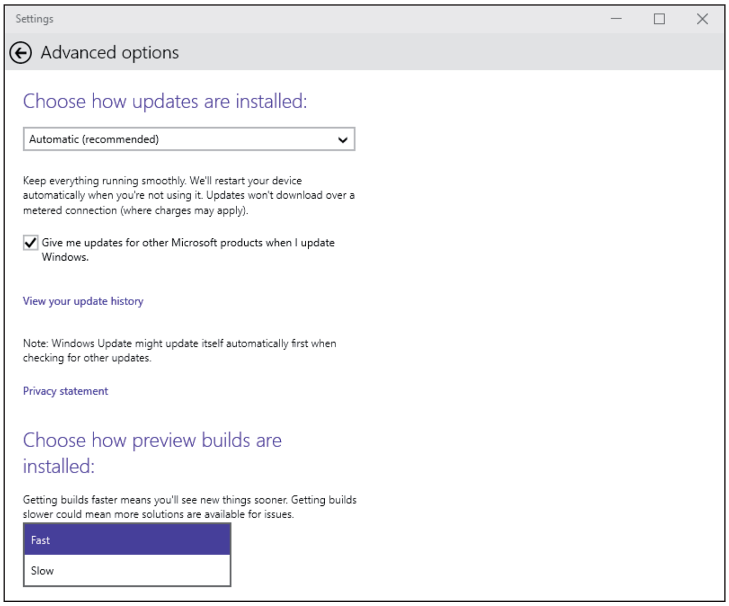
- Consumers and anyone else not running enterprise versions of *Windows 10* could be receiving less well tested and perhaps even beta-quality code as part of their *Windows 10* updates. And while home users and small businesses may not run 24×7 mission-critical systems that require 100% availability, they may be running systems which are critical to them, and running unstable code on their computers may cause crashes, performance problems and other issues preventing them from using their computers for work and play.
- Enterprises, on the other hand, may have to wait a while longer for *Microsoft* to signal the 'all clear' on patches until they have received enough testing by *Microsoft*'s consumer 'guinea pigs' for them to be marked as ready for enterprise deployment. Attackers, meanwhile, suffer no such delays and can begin creating exploits immediately to target vulnerabilities that have yet to be patched in *Windows 10 Enterprise*.

It is also important to keep in mind that *Microsoft's* assessment of the impact of a vulnerability may be different from the actual impact it has in your organization. *Microsoft* makes use of both a Security Rating System [7] and an Exploitability Index [8] in order to help determine impact. While these assessments are generally accurate for the majority of *Microsoft*'s customers, there will be enterprises that are at higher risk due to the way in which the technologies are deployed and used throughout the business. Conversely, there will be some enterprises that are at lower risk for the same reason.

## GOOD PATCH, BAD PATCH

The question of patch quality is key here. Last year and in early 2015, there were several occasions on which *Microsoft* released updates for *Windows* only to receive numerous reports of problems from customers – some of which were so severe that *Microsoft* had to pull the updates until they themselves could be updated (see Table 1).

*Microsoft* has certainly indicated that *Windows 10* will receive updates and new features more quickly, but it is still an open question as to what this means for *Windows 10*'s quality, let alone its reliability and resiliency.



Settings

Advanced options

Choose how updates are installed:

Automatic (recommended)

Keep everything running smoothly. We'll restart your device automatically when you're not using it. Updates won't download over a metered connection (where charges may apply).

☑ Give me updates for other Microsoft products when I update Windows.

View your update history

Note: Windows Update might update itself automatically first when checking for other updates.

Privacy statement

Choose how preview builds are installed:

Getting builds faster means you'll see new things sooner. Getting builds slower could mean more solutions are available for issues.

Fast

Slow

*Figure 1: Windows 10 Enterprise Technical Preview Build 9926 showing 'fast' and 'slow' release channels.*

## RECOMMENDATIONS

Until we have evidence of how *Windows 10*'s new patching strategy works in the real world, it is recommended that the following steps be taken:

- Continue testing and evaluating *Windows 10* in your environment. Regardless of whether you decide to deploy it immediately or wait, continuing to familiarize

| Month | Patch |
|---|---|
| July 2014 | MS14-037: Cumulative security update for Internet Explorer: July 8, 2014 [9]<br>*(Broke Flexera InstallShield [10] and Dell Encryption software [11])* |
| August 2014 | MS14-045: Description of the security update for kernel-mode drivers: August 12, 2014 [12]<br>Update to support the new currency symbol for the Russian ruble in Windows [13]<br>August 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 [14]<br>August 2014 update rollup for Windows RT, Windows 8, and Windows Server 2012 [15]<br>*(0x50 STOP error; issues with managing fonts; issues with displaying fonts; issues with displaying application windows)* |
| September 2014 | Vulnerabilities in Microsoft Lync Server Could Allow Denial of Service (2990928) [16]<br>*(Update failed to install correctly and had to be replaced, twice)* |
| October 2014 | Availability of SHA-2 Hashing Algorithm for Windows 7 and Windows Server 2008 [17]<br>*(Prevented Windows from booting)* |
| December 2014 | Update Rollup 8 for Exchange Server 2010 Service Pack 3 (KB2986475) [18]<br>*(Broke Outlook's connection to a specific version of Exchange)* |
| February 2015 | PowerPoint 2013 Update (KB2920732) – February 2015 [19]<br>*(Prevented PowerPoint 2013 from running on Windows RT devices)* |

*Table 1: Microsoft released several updates for Windows only to receive numerous reports of problems from customers.*

yourself with its new features will help ensure that your rollout goes more smoothly.

- Since the effect of *Microsoft*'s new patching schema won't be known until sometime after *Windows 10* has become generally available, hold off with deployment until you can determine whether this makes *Windows 10* more secure or less secure than the operating system(s) it is replacing.

  If the delay in enterprise updates results in the attack surface increasing, you may be better off staying on an older enterprise version of *Windows* that receives updates sooner than *Windows 10*'s enterprise version.

- Another approach worth considering would be to change how update rollouts are staged in your organization: in many organizations, it is common to test *Windows* updates across a small percentage of users (often 10%) before rolling out across the entire enterprise.

  Consider increasing the initial rollout to a slightly higher number, such as 15% of users, followed by a second phase of rollouts to another 25–33% before globally deploying updates to all users. Adding a second wave of testers can help detect issues not discovered during the first wave of deployment, as well as helping to pinpoint issues discovered in that first wave.

  All too often, the initial phases of a rollout involve a company's most technical users (IT, R&D engineering and so forth), not taking into account users from other departments who often have specialized use cases. Make sure your test waves include users from all departments and at all computing skill levels. Broadening your testing to include additional categories of users will increase the chances of identifying problems before the global rollout.

- While each new version of *Windows* brings enhanced security mechanisms, determined adversaries will up their game as well. Deploy anti-malware software that uses a variety of techniques beyond simple signature-based detection, including heuristics, emulation, HIPS [20], exploit-blocking and SIGINT in order to protect endpoints.

- If an attacker should breach your network's perimeter, there are still steps you can take to slow their movement through the network as well as limit their access to useful intelligence:

  - implement multi-factor authentication for access to sensitive data
  - encrypt sensitive data stored on endpoints.

- Finally, and this is more of a general rule than one specific to *Windows 10*, implement a backup methodology that works for your organization, and verify periodically that it works.

## CONCLUSION

Over the past years, we have seen attacks increase against all platforms, not just *Microsoft*'s. As a matter of fact, one might even argue that such attacks are a sign of success: it means the platform is now large enough for attackers to see value in targeting it. We cannot say for certain what the overall impact of *Windows 10*'s new patching strategy will be on the security of businesses that adopt it, and we won't be able to assess the situation until some time after *Windows 10* has established itself in the enterprise. And, of course, there's no guarantee that simply being a more secure version of *Windows* [21] (as *Windows 8* was in comparison with *Windows 7*, or even *Windows 8.1* was in comparison with *Windows 8.0* [22]) will mean widespread adoption, either.

## REFERENCES

[1] Goretsky, A. Make 2015 More Secure: Lessons from 2014. BrightTALK. https://www.brighttalk.com/webcast/1718/125051.

[2] Zero day. Virus Radar. http://virusradar.com/en/glossary/zero-day.

[3] Alkove, J. Windows 10 for Enterprise: More secure and up to date. Windows for your Business. http://blogs.windows.com/business/2015/01/30/windows-10-for-enterprise-more-secure-and-up-to-date/.

[4] Long-term support. Wikipedia. http://en.wikipedia.org/wiki/Long-term_support.

[5] LTS. Ubuntu wiki. https://wiki.ubuntu.com/LTS.

[6] Mozilla Firefox ESR overview. https://www.mozilla.org/en-US/firefox/organizations/faq/.

[7] Security Bulletin Severity Rating System. Security TechCenter. https://technet.microsoft.com/en-us/security/gg309177.aspx.

[8] Microsoft Exploitability Index. Security TechCenter. https://technet.microsoft.com/en-us/security/cc998259.

[9] MS14-037: Cumulative security update for Internet Explorer: July 8, 2014. https://support.microsoft.com/kb/2975687.

[10] Microsoft's Security Update – Impact on InstallShield and InstallShield for AdminStudio (KB2962872). http://www.flexerasoftware.com/landing/Microsoft-Security-Update-IS-AR-KB2962872.html.

[11] Paoli, C. InstallShield and Dell Encryption Crashes Connected to July Security Patch. Redmond Magazine. http://redmondmag.com/articles/2014/07/15/july-security-patch-issues.aspx.

[12] MS14-045: Description of the security update for kernel-mode drivers: August 12, 2014. http://support.microsoft.com/kb/2982791.

[13] Update to support the new currency symbol for the Russian ruble in Windows. http://support.microsoft.com/kb/2970228.

[14] August 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2. http://support.microsoft.com/kb/2975719.

[15] August 2014 update rollup for Windows RT, Windows 8, and Windows Server 2012. http://support.microsoft.com/kb/2975331.

[16] August 2014 update rollup for Windows RT, Windows 8, and Windows Server 2012. https://technet.microsoft.com/en-us/library/security/ms14-055.aspx.

[17] Microsoft Security Bulletin MS14-055 – Important. Vulnerabilities in Microsoft Lync Server Could Allow Denial of Service (2990928). https://technet.microsoft.com/en-us/library/security/2949927.

[18] Update Rollup 8 for Exchange Server 2010 Service Pack 3. http://support.microsoft.com/kb/2986475.

[19] PowerPoint 2013 Update (KB2920732) – February 2015. http://blogs.technet.com/b/office_sustained_engineering/archive/2015/02/13/powerpoint-2013-update-kb2920732-february-2015.aspx.

[20] HIPS. Virus Radar. http://virusradar.com/en/glossary/hips.

[21] Goretsky, A. A white paper: Windows 8’s Security Features. We Live Security. http://www.welivesecurity.com/2012/10/09/windows-8s-security-features/.

[22] Goretsky, A. Windows 8.1 – security improvements. We Live Security. http://www.welivesecurity.com/2013/11/17/windows-8-1-security-improvements/.

**Editor:** Martijn Grooten

**Chief of Operations:** John Hawes

**Security Test Engineers:** Scott James, Tony Oliveira, Adrian Luca

**Sales Executive:** Allison Sketchley

**Editorial Assistant:** Helen Martin

**Consultant Technical Editors:** Dr Morton Swimmer, Ian Whalley

**© 2015 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England.**

**Tel: +44 (0)1235 555139. Fax: +44 (0)1865 543153**

**Email: editorial@virusbtn.com**

**Web: http://www.virusbtn.com/**