SIM2K
Adapting Technology to Your Business Needs

10•19
Information you can use

SIMformation

Microsoft Causing Questions on W10 Updates

Since Microsoft gave its Windows 10 update model another shake-up over the Summer, the IT world has tried to parse Microsoft's intentions for demoting this fall's intended feature upgrade, dubbed Windows 10 1909, to little more than a rerun of May's release. It seems that five questions remain unanswered that are the most important to enterprises and IT administrators. Once Microsoft releases 1909 — which should be soon — perhaps some will be resolved.

Is 1909 a one-timer — or the new fall normal?

There's little chance Microsoft invested as much time and energy as it did in creating a completely different kind of upgrade, serviced using a different mechanism than before, only to use the results just once. Doing so would be idiocy when other less costly, less disruptive avenues were available, including skipping the refresh entirely or extending support for, say, Windows 10 1809 or even Windows 10 1903 to cover for the omitted update.

If that's indeed the case, commercial customers need assurance from Microsoft that 1909's format and delivery will be the norm for each fall upgrade. Businesses require a definitive schedule and information on an update's contents – for the latter, at least a sense of the quantity of change – for planning purposes.

Will Microsoft move to a single upgrade annually?

It certainly appears that the company has positioned its Windows update and upgrade model to do that, for there's little space between an "upgrade" with a smattering of new features and one with no new features. They just tighten the feature spigot that last half a turn to shut it off completely. It's clear, for the moment at least, that Microsoft remains committed to a pair of Windows 10 upgrades each year, even if one is such in name only. Whether Microsoft's stance is due to pride in a promise or for something more tangible is less clear.

A once-a-year upgrade would require more rearranging, not that there's anything wrong with that. The 30-month support lifecycle for Windows 10 Enterprise (and Education) would require shifting to the spring upgrade if the fall update was eliminated. Labeling might change (what purpose would yy03 have when there was no yy09?), perhaps to Windows 10.21 for the year after next. After all, Microsoft is the odd man out. Other OS makers, such as Apple and Google, have annual refreshes, whether on personal computers or mobile devices. Microsoft may well oblige.

Has Microsoft dumped the signaling to commercial customers that a feature upgrade is business ready?

It sure seems that way. Up to Windows 10 1809, the initially-crippled 2018 feature upgrade delayed by months, Microsoft gave businesses a green light when it (Microsoft) believed the code had been shaken out by early adopters and those forced into installing the upgrade, such as Windows 10 Home users. The business-ready flare went up several months after the upgrade's debut. Microsoft hasn't said a word about Windows 10 1903, which appeared May 21 and so is now four months old.

One side says Microsoft won't bother with such notifications as evidenced from Microsoft's quashing of the Semi-Annual Channel (SAC) milestone that marked an upgrade's reliability for commercial customers to its harping at enterprises to begin their upgrade process as soon as the code launches. On the other hand, Microsoft did say it would continue to offer this good-to-go declaration.

Because 1909 is a cumulative update of 1903 – for those old enough to remember, a "service pack" in earlier Microsoft-ese – and its contents are, in fact, identical to a fixed-up 1903, 1909 has, theoretically, been as well tested as has 1903. And Windows 10 1909's target release was to be in September, whose end has passed. Even if delayed into October, the launch of 1909 would be within days of any business-readiness alert for 1903 that Microsoft might give this late in the process.

Is it 1903 or 1909 on your PC?

Once an organization has 1909 in place — probably through upgrading from a pre-1903 version of Windows 10 — it will have to keep in mind that the KB designations for the two are identical. As long as it's assigning the cumulative update to machines running one of those two versions, however, it won't matter, as the contents of the update for each are identical. Microsoft could alleviate some of the bewilderment by better explaining how the cumulative update process works on end points, whether Windows 10 Pro or Windows 10 Enterprise. Perhaps that will happen at the same time it rolls out 1909.

Will Microsoft initially defer 1909's new features? If so, will it let enterprises control or even permanently disable them?

Windows 10 1909 has been tested differently than past upgrades: Initially, Microsoft fed the update to Insider participants with the new features switched off. Later, it first enabled the features – they're neither large in number or in import – for a portion of the pool, then for all. But Microsoft has never said whether 1909 will ship in the same way.

If Microsoft in fact utilizes Windows 10 1909 as the business-ready version of 1903, setting new features to off would also mean companies would not have to test or prep for them. Instead, they'd be dealing with the changes baked into Windows 10 only up to and including 1903's, just as if they'd migrated to that version.

If Microsoft inhibits 1909's new features at launch, it is unclear when it will turn them on. Will all go live at once or will Microsoft flip the switch on some now, others later? How will it decide that? Microsoft needs to answer these questions and more.

As you can see, Microsoft has created more questions than answers concerning updates to Windows 10. That is why SIM2K is here to provide you with advice on the "go or no go" on updates. We vet all releases from Microsoft ourselves before applying these for our Managed Update clients, or pronounce them OK for all others to apply. Your Support Team will keep you apprised of time to update your Windows 10 machines. Call us with questions.

Microsoft Excel Keyboard Shortcuts

Last month we covered keyboard shortcuts for Word, and had a request for the same covering Excel spreadsheets. So, here are the most frequently used shortcuts.

Formatting
ctrl+1 Format cells dialog box
ctrl+5 Strikethrough
ctrl+B Bold
ctrl+I Italic
ctrl+U Underline
shift+ctrl+` General format
shift+ctrl+1 Format cell to two decimal places
shift+ctrl+2 Format cell to time
shift+ctrl+3 Format cell to date
shift+ctrl+4 Format cell to currency
shift+ctrl+5 Format cell to percentage
shift+ctrl+6 Format cell to scientific notation
shift+ctrl+7 Draws outline around your selection

Cell Selection
ctrl+A Select All Cells in range
shift+F8 Add to selection
ctrl+[SPACE] Select the current column
shift+[SPACE] Select the current row
shift+HOME Select to beginning of row
shift+END↵ Select to last used cell in row
shift+ctrl+HOME Select to beginning of worksheet
shift+ctrl+END Select to end of worksheet
shift+ctrl+8 Select data region surrounding active cell
shift+ctrl+O Select all cell containing a comment
ctrl+[Select cells that formula directly references
ctrl+] Select formula that references the active cell

Data
shift+ctrl+; Insert Current Time
ctrl+; Insert Current Date
ctrl+C Copy
ctrl+V Paste
ctrl+X Cut
ctrl+Y Repeat
ctrl+Z Undo
shift+F2 Edit cell comment
ctrl+BACKSPACE Display the active cell
alt+IC Insert column
alt+IR Insert row
ctrl+D Fill Down
ctrl+R Fill Right
shift+ctrl+= Insert Cells, Rows, Columns
shift+ctrl+F3 Create name using row and column labels
F2 Edit

Workbooks
ctrl+0 Hide columns
ctrl+9 Hide rows
ctrl+F10 Maximize or restore window
ctrl+F9 Minimize workbook
shift+ctrl+9 Unhide rows
F7 Spell check

Formulas
alt+= AutoSum
ctrl+' Copy formula from cell above
alt+ctrl+F9 Forces full calculation of all worksheets
shift+ctrl+A Insert argument names into formula
F3 Paste Name
shift+F3 Paste function into formula
shift+ctrl+' Copy value from cell above

General
alt+F1 Insert a Chart sheet
alt+F11 Open Visual Basic Editor
alt+F8 Macro dialog box
shift+alt+F2 Save Workbook
ctrl+F11 Inset 4.0 Macro sheet
shift+F10 Display shortcut menu

Navigation
ctrl+END Move to last used cell in a worksheet
ctrl+G Goto
ctrl+HOME Move to the first non-header cell of the sheet
F6 Next Pane
shift+↵ Go to previous cell
shift+F6 Previous Pane
HOME Move to beginning of row
↵ Move down a cell in selected range
shift+↵ Move up a cell in selected range
ctrl+. Move from corner cell to corner cell in range
↵ Go to next cell

Misc
F10 Activate menu
ctrl+6 Show/Hide objects
ctrl+7 Show/Hide Standard toolbar
ctrl+8 Toggle Outline symbols
ctrl+↵ Fill the selected cell range with the current entry.
ctrl+F Find
ctrl+F12 File Open
ctrl+H Replace
ctrl+O Open
F9 Recalculate all workbooks
shift+ctrl+F Font Drop Down List
shift+ctrl+FF Fill tab of Format Cell Dialog box
shift+ctrl+P Point size Drop Down List
shift+F4 Find Next
shift+F9 Re-calculate active worksheet
TAB Next tool

Happy Calculating!

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

What Ails the PC Industry?

Computerworld recently ran this discussion on what is holding back growth in the current PC market. Here is a synopsis of the author's consideration of this issue.

There are three problems currently reducing market growth. While this isn't an exhaustive list by any means, fixing these three would not only increase growth, they would improve our satisfaction and excitement regarding this segment. The three issues are the lack of a standard cross-vendor processor socket, the lack of a recognized way to measure security across vendors and the lack of an industry effort to drive advanced PC innovation.

Common socket
At one time, both Intel and AMD used a common socket, which meant that if one vendor had problems, an OEM could easily switch to the other vendor. The creation of AMD as a processor vendor was largely because Intel needed a peer so that their large customers wouldn't be dependent on one vendor. This common socket was negotiated away in the 1990s without OEM influence or support, and it substantially weakened the industry by preventing the one critical thing they demanded when X86 first became a thing: a plug-compatible, two-vendor solution. This common socket was a primary requirement during the birth of the PC industry. Those that set the requirement never agreed to its removal, and having it makes the entire industry healthier.

Security
Currently HP leads the PC market in security and, typically, that would drive a bit of a security arms race. This arms race is critical given the threat level is increasing and the costs and penalties associated with a breach are reaching astronomical levels. But, without a common way to measure security, that competition hasn't evolved – and the competing vendors honestly don't seem to believe they are dropping behind. To preserve the industry and adequately protect buyers there really needs to be an industry-standard way to rank the various security efforts and assure they apply to not only commercial but to consumer lines. Typically, because we tend to focus on blame and not remediation when there's a large breach, the OEM shares a significant level of exposure for this practice with IT. Without a common way to measure security, this exposure only shows up in private post-breach reviews, preventing adequate mitigation. Additionally, increased security is often in hardware, not software, and requires a hardware upgrade. A more modular approach should mitigate this exposure, but the effort likely won't get funding unless a common benchmark points it out.

Centralized advanced PC innovation
There was a lot of innovation during the first two decades of the PC's life. Efforts to create modular solutions, more interesting designs, more robust cases and even more aggressive use of water cooling have all but died out at an industry level. That's held back industry innovation and created a higher risk associated with individual innovation with the OEMs. If we want to grow the market, there needs to be less risk and more focus on applying breakthroughs to create ever more interesting products so that the industry can drive churn.

These three things would make the PC segment more interesting, lucrative and safe and reverse the stagnation that has plagued the market in the last decade or so. The PC market can and should be more lucrative, more interesting and safer than it is. And it's in all of our best interests that it again evolves back to what it once was.

"Random Tid-Bytes"

Dropbox Now More than Just File Sharing Hub

Dropbox has launched a collaboration hub designed to let users work together around a variety of documents, moving towards the company's goal of becoming more focused on productivity. Called Dropbox Spaces, it acts as a shared folder for teams that combines documents from a range of sources into one place, with the ability to chat with colleagues and assign tasks. It will also connect with various third-party video and text communication platforms. The rollout of Spaces edges the company into closer competition with the likes of Slack, Microsoft Teams and other vendors that all aim to be the central app employees spend most of their day using. In addition to announcing the availability of Spaces, Dropbox offered details of new features to come. That list includes integration with Dropbox Paper, the company's collaborative word processing tool, which will be accessible alongside Google Docs and Microsoft Office files in Spaces. Also on the way: integration with Atlassian's popular work management application, Trello, that lets users add Dropbox content to Trello cards, and integration with e-signature app, HelloSign.

Zultys Releases New Phone

ZIP 45G, an advanced Gigabit IP business phone. ZIP 45G will start shipping and be fully supported on Release 14.0.6 and later via patches by the end of this week.
The ZIP 45G features include:

- Full duplex speakerphone
- Dual Gigabit Ethernet ports
- 21 Programmable keys
- USB and Bluetooth Headset support (optional adapter required)
- Electronic Hook Switch (EHS) support
- Busy Lamp Field (BLF)
- Wi-Fi support (optional adapter required)

The ZIP 45G supports wired and wireless headsets, including Electronic Hook Switch functionality when used with compatible USB and Bluetooth headsets. The optional ZIP 450M Expansion Module supports additional programmable keys. The phone is fully compatible with Zultys' ZAC and MXIE Unified Communication applications, allowing users to manage calls and messages directly from their computer.

Emergency Patch for IE

Microsoft released an emergency security update to patch a vulnerability in Internet Explorer (IE), the legacy browser predominantly used by commercial customers. The flaw has already been exploited by attackers, making it a classic "zero-day," a vulnerability actively in use before a patch is in place. Microsoft said the malware is a remote code vulnerability, meaning that a hacker could, by exploiting the flaw, introduce malicious code into the browser. Remote code vulnerabilities are among the most serious. That seriousness, as well as the fact that criminals are already leveraging the vulnerability, was reflected in Microsoft's decision to release an emergency patch outside of the regular update cycle the company follows.

What You Need to Know About Exploits

Have you ever noticed how software developers are forever patching and updating their software – sometimes releasing updates mere days after the initial software release? That's because every piece of software you own and will ever own in your life will have vulnerabilities cybercriminals can find and take advantage of – in other words, "exploit." There is no such thing as exploit-free software – there will always be holes.

By way of exploits, cybercriminals can gain access to your computer and steal sensitive information or install malware. Despite a slow-down in exploit activity, cybercriminals are continuing to fall back on this stealthy method of attack.

What is an exploit?

A computer exploit is a type of malware that takes advantage of bugs or vulnerabilities, which cybercriminals use to gain illicit access to a system. These vulnerabilities are hidden in the code of the operating system and its applications just waiting to be discovered and put to use by cybercriminals. Commonly exploited software includes the operating system itself, browsers, Microsoft Office, and third-party applications. Sometimes exploits are packaged up by cybercriminal groups into what's called an exploit kit. Exploit kits make it easier for criminals with limited technical knowledge to use exploits and spread malware.

Exploit attacks often start with malspam and drive-by downloads. Cybercriminals trick unsuspecting victims into opening an infected email attachment or clicking links that redirect to a malicious website. Infected attachments, often a Word document or PDF, will contain exploit code designed to take advantage of application weaknesses.

Drive-by downloads take advantage of vulnerabilities in your browser, like Internet Explorer or Firefox for example, or the plug-ins running within your browser such as Flash. You may visit a website you've visited safely in the past, but this time the website has been hacked and you won't even know it. Alternatively, you may click a malicious link in a spam email that takes you to a spoofed version of a familiar website. And in particularly tricky instances, you may visit a legitimate website displaying an advertisement or pop-up infected with malware – also known as malvertising. Upon visiting the site, malicious code on the webpage will work invisibly in the background to load malware onto your computer.

Cybercriminals use exploits as a means to some malicious end, ranging from annoying problem to crippling nuisance. Cybercriminals may try to put your computer's resources to work in a zombie botnet for the purposes of a DDoS attack or to mine Bitcoin (cryptojacking). Alternatively, cybercriminals may try to install adware and flood your desktop with ads. Cybercriminals may want to get on your system and steal data outright or install malware to secretly collect data from you over time (spyware). Finally, cybercriminals may install malware that encrypts all your files and demand payment in exchange for the encryption key (ransomware).

Proactively looking for exploits has become a sport for some hackers. At the annual Pwn2own competition, exploit experts earn cash and prizes for successfully hacking into popular software across multiple categories, including web browsers and enterprise applications. As a demonstration of their interest in software security, Microsoft and VMware sponsored the Pwn2own event in 2018.

Here are a few tips if you want to get proactive about exploit protection.

Stay up-to-date. Do you regularly update your operating system and all the various applications you have installed? If you answered no, you might be a potential victim for cybercriminals. After a zero-day exploit becomes known to the software vendor and a patch is released, the onus is upon the individual user to patch and update their software. In fact, zero-day exploits become more dangerous and widespread after they become public knowledge, because a broader group of threat actors are taking advantage of the exploit. Check back with your software providers and see if there are any updates or patches available. If possible, go into your software settings and turn auto-updates on so these updates happen automatically in the background without any extra effort on your part. This will eliminate the amount of lag time between when a vulnerability is announced and when it's patched. Cybercriminals prey on people who forget or just don't know to update and patch their software.

Upgrade your software. In some cases, a software application becomes so old and unwieldy the software maker stops supporting it, which means any additional bugs that are discovered will not be fixed. As per the previous recommendation, make sure your software is still supported by the maker. If it isn't, upgrade to the latest version or switch to something else that does the same thing.

Stay safe online. Make sure Microsoft SmartScreen or Google Safe Browsing are enabled for your web browser of choice. Your browser will check every site you visit against the blacklists maintained by Microsoft and Google and steer you away from sites known to dish up malware. Effective anti-malware tools like SIM2K MAVerick will also block bad sites, offering you multiple layers of protection.

Use it or lose it. If there's no software, there's no vulnerability. If you aren't using the software anymore, delete it from your computer. Hackers can't break into something that isn't there.

Use anti-exploit software. A zero-day exploit is a software vulnerability only the cybercriminals know about. There's not much we can do to protect ourselves from the threats we don't know. However, SIM2K installs Cylance protection for our clients that is designed to detect malware, even for zero-day exploits, to help protect your data.

Good endpoint security software is an essential part of any exploit protection program. SIM2K has a variety of tools to help protect you like MAVerick and Cylance, as well as SIM2K StickyNet anti-spam to ferret out malware e-mails. We recommend that everyone conduct a periodic audit of their security plan and anti-exploit software. Call us for more information on how we can help you.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com