SIM2K
Adapting Technology to Your Business Needs

7•21
Information you can use

SIMformation

Windows 11 Is Coming

So much for that promise – the one Microsoft made six years ago when it told customers that Windows 10 was "the last version of Windows" they would see. Instead, Windows 10 will end in late 2025, its 10-year lifecycle the same as Microsoft's previous operating systems, replaced by the next-in-line numeral and numeric label – Windows 11.

Details remain somewhat sketchy, but it is expected that Windows 11 won't be an exact copy of Windows 10, renamed. Or renumbered.

Microsoft has confirmed: For a time, both Windows 10 and Windows 11 will be in play. "As you make the move to Windows 11, we will continue to support you as you use Windows 10." In other words, as Windows 7 was to Windows 10, so will Windows 10 be to Windows 11. Both will receive monthly security updates, the hallmark of Microsoft's support policies. There will be a feature upgrade later in the year, Microsoft said, labeling it 21H2. It will come with the standard 30 months of support on devices running Windows 10 Enterprise or Windows 10 Education. At the same time, Microsoft will drop Windows 10's twice-a-year upgrade cadence and replace it with a once-yearly feature upgrade for Windows 11 that launch in each year's second half.

Windows 11 will come only in a 64-bit edition, unlike Windows 10, which has been available in both 32- and 64-bit versions. 32-bit applications will continue to run and work on Windows 11, but devices with a 32-bit processor will not be able to install the operating system. That shouldn't be much of a burden, seeing that those CPUs fell by the wayside a decade and more ago. Customers running Windows 10 under a legal license can move to Windows 11 free of charge. As far as Microsoft is concerned, Windows 11 is simply another feature upgrade for Windows 10.

"Microsoft 365 licenses that include Windows 10 licenses will permit you to run Windows 11 on supported devices," Microsoft said on its support site. "If you have a volume license, it will equally cover Windows 11 and Windows 10 devices before and after upgrade." Unlike the free Windows 7-to-10 upgrade offer Microsoft extended in 2015, there is no time limit on the 10-to-11 deal, at least at the outset. "Upgrading to Windows 11 is similar to taking a Windows 10 feature update," asserted Microsoft.

So what can you expect from Windows 11? Here are some changes and improvements:

- A new, more Mac-like interface. Windows 11 features a clean design with rounded corners, pastel shades and a centered Start menu and Taskbar.
- Integrated Android apps. Android apps will be coming to Windows 11 and installable from within the new Microsoft Store via the Amazon Appstore.
- Widgets. While they've been around for a while, you can now access widgets directly from the Taskbar and personalize them to see whatever you like.
- Microsoft Teams integration. Teams is getting a face-lift and will be integrated directly into the Windows 11 Taskbar, making it easier to access (and a bit more like Apple's FaceTime). You'll be able to access Teams from Windows, Mac, Android or iOS.
- Xbox tech for better gaming. Windows 11 will get certain features found in Xbox consoles, like Auto HDR and DirectStorage, to improve gaming on your Windows PC.
- Better virtual desktop support. Windows 11 will let you set up virtual desktops in a way that's more similar to MacOS, toggling between multiple desktops for personal, work, school or gaming use.
- Easier transition from monitor to laptop, and better multitasking. The new OS includes features called Snap Groups and Snap Layouts – collections of the apps you're using at once that sit in the Taskbar, and can come up or be minimized at the same time for easier task switching. They also let you plug and unplug from a monitor more easily without losing where your open windows are located.

Windows 11 is now available as an Insider Preview build download for those in the Windows Insider Program, and will be available as a public beta this month. It will begin rolling out to all compatible PCs and new PCs around the 2021 holiday season, according to Microsoft, and will continue rolling out into 2022. However, several hints suggest that Windows 11 could arrive as early as October.

This release also ends the push for Windows to be "Software as a Service" (SaaS). Microsoft had big plans for Windows 10. The operating system would not be the next upgrade from Windows 7 but would be the final version for the rest of time. Rather than replace Windows 7 with another edition that would eventually age out of support and be supplanted in turn by Windows 10+x, Windows 10 would be constantly refreshed, with new features and functionality added to major updates released first three, then two times a year. The retreat from multiple yearly upgrades makes it hard to believe Microsoft can call this a "service"when refreshes occur only once every 12 months. Once a year is not a service, it's a subscription.

As with any "new" operating system, SIM2K does not recommend immediately upgrading your PC. There are always some issues that arise from a new OS, either from operations or interactions with legacy programs unique to your office, so don't be in a hurry to download Windows 11. SIM2K will work with you to first evaluate how it might impact your network environment, and then develop a roll-out plan for your office. Call us for details.

LinkedIn Breached Again

LinkedIn has reportedly been breached – again –following reports of a massive sale of information scraped from 500M LinkedIn user profiles in the underground in May. According to Privacy Shark, the VPN company who first reported on this incident, a seller called TomLiner showed them he was in possession of 700 million Linkedin user records. That means almost all (92%) of LinkedIn's users are affected by this.

RestorePrivacy, an information site about privacy, examined the proof the seller put out and found the following information, scraped from LinkedIn user profiles:

- E-mail addresses
- Full names
- Phone numbers
- Physical addresses
- Geolocation records
- LinkedIn username and profile URL
- Personal and professional experience/background
- Gender
- Other social media account usernames

Note that account credentials and banking details don't appear to be part of the proof. This suggests that the data was scraped rather than breached. Scraping happens when somebody uses a computer program to pull public data from a website, using the website in a way it wasn't intended to be used. Each individual request or visit is similar to a real user visiting a web page, but the sum total of all the visits leaves the scraper with an enormous database of information.

To scrape all this information, the seller abused LinkedIn's API, a similar tactic to the one used in the almost-as-enormous April LinkedIn and Facebook breachs.

LinkedIn claims there is really no breach: "While we're still investigating this issue, our initial analysis indicates that the dataset includes information scraped from LinkedIn as well as information obtained from other sources. This was not a LinkedIn data breach and our investigation has determined that no private LinkedIn member data was exposed. Scraping data from LinkedIn is a violation of our Terms of Service and we are constantly working to ensure our members' privacy is protected."

But this is still a serious issue for your privacy. Having your e-mail address or contact number available for everyone to see is risky. If they know these two things, you can be a candidate target for spam campaigns: email, SMS, and robocalls. To make matters worse, the more that scammers know about you, the more plausible and enticing they can make their messages for, and the easier it is for them to pretend to be you when scamming others.

If you're a LinkedIn user, and you're worried about the possible repercussions, now is a good time to take the time to sit down and audit your LinkedIn profile.Start with security: Make sure you have two-factor authentication (2FA) enabled. Take a look at your LinkedIn profile and decide which bits of it you'd rather make private. Remember that you, as a LinkedIn user, can decide which information to show or hide, and who gets to see them.

Kaseya Ransomware Attack

Just in time to ruin the July 4th weekend, ransomware attackers used Kaseya – a software platform designed to help manage IT services remotely – to deliver their payload. Sophos reported that affected systems will demand $44,999 to be unlocked. A note on Kaseya's website implores customers to shut off their VSA servers for now "because one of the first things the attacker does is shutoff administrative access to the VSA." According to reports, the attack targeted six large MSPs and has encrypted data for as many as 200 companies.

Kaseya issued another update, saying that it had been advised by its outside experts that "customers who experienced ransomware and receive a communication from the attackers should not click on any links – they may be weaponized." The attack works with REvil ransomware arriving via a Kaseya update and using the platform's administrative privileges to infect systems. Once the Managed Service Providers are infected, their systems can attack the clients that they provide remote IT services for (network management, system updates, and backups, among other things). In a statement, Kaseya said "We are investigating a potential attack against the VSA that indicates to have been limited to a small number of our on-premises customers only." A notice claims that all of its cloud servers are now in "maintenance mode," a move that the spokesperson said is being taken due to an "abundance of caution."

As events unfolded, Kaseya issued a statement saying they estimated the number of MSPs affected is fewer than 40, and was preparing a patch to mitigate the vulnerability. "While our early indicators suggested that only a very small number of on-premises customers were affected, we took a conservative approach in shutting down the SaaS servers to ensure we protected our more than 36,000 customers to the best of our ability," adding that the company's SaaS customers were never at risk, and reiterating that "only a very small percentage of our customers were affected." The attackers demanded $70 million, and claimed they infected over a million devices

Bloomberg reported that the attack was affecting more than 1,000 businesses in a ripple effect; the attack focused on managed service providers, but these providers offer IT services to other companies that may now be affected as well. A grocery chain in Sweden reported it couldn't open 800 of its stores on Saturday when the attack resulted in its cash registers malfunctioning.

The attack has been linked to the notorious, REvil ransomware gang (already linked to attacks on meat supplier JBS earlier this year). REvil has previously been linked with Russia. Reuters reports that the REvil affiliate behind the attack "has indicated a willingness to temper their demands in private conversations with a cybersecurity expert and with Reuters." According to the news organization, the attackers said they were prepared to lower the asking price for a universal decryptor from $70 million to $50 million. A universal decryptor could be used to free all of the victims—all the customers of Kaseya's customers—and save the attackers the bother of negotiating with each of up to 1,500 victims separately. It is unknown (to date) if Kaseya will meet these demands.

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 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

China Behind Microsoft Hack

The US and other nations have pointed to China for a wide range of "malicious cyber activities" – including a massive hack of Microsoft's e-mail service earlier this year that exposed the private information of thousands of Americans. The White House accused China of fostering "an intelligence enterprise that includes contract hackers who also conduct unsanctioned cyber operations worldwide," blaming the country's Ministry of State Security for everything from ransomware attacks and extortion to cryptocurrency heists and "rank theft."

In particular, the US slammed China for a breach of Microsoft's Exchange email service that was first disclosed this March. In the breach, hackers associated with the Ministry of State Security accessed thousands of e-mail accounts associated with businesses, government offices and schools around the world, according to the White House. The hack likely "netted high-value espionage targets," the Wall Street Journal reported at the time.

The official warning stated that the National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China state-sponsored malicious cyber activity is a major threat to U.S. and Allied cyberspace assets. Chinese state-sponsored cyber actors aggressively target U.S. and allied political, economic, military, educational, and critical infrastructure personnel and organizations to steal sensitive data, critical and emerging key technologies, intellectual property, and personally identifiable information. Some target sectors include managed service providers, semiconductor companies, the Defense Industrial Base, universities, and medical institutions. These cyber operations support China's long-term economic and military development objectives.

Meanwhile, the Justice Department announced charges against four Chinese nationals who prosecutors said were working with the Ministry of State Security in a hacking campaign that targeted dozens of computer systems, including companies, universities and government entities.

A DoJ Spokesman said "These criminal charges once again highlight that China continues to use cyber-enabled attacks to steal what other countries make, in flagrant disregard of its bilateral and multilateral commitments. The breadth and duration of China's hacking campaigns, including these efforts targeting a dozen countries across sectors ranging from health care and biomedical research to aviation and defense, remind us that no country or industry is safe."

The CISA released a 31-page document outlining ways to combat the PRC's hacking attempts. In a nutshell, it reinforces what SIM2K is urging all of our clients to do – update all software to current versions; install the latest in preventive detection tools; use multi-factor authentication on accounts, especially for any remote access tools; consider VPNs over Remote Desktop access; train staff to recognize phishing attacks and ransomware ploys. Contact us for more information on how to protect your network from malicious attacks, be it from China or other bad actors.

"Random Tid-Bytes"

Watch Out for Pandemic "Re-Opening" Attacks

As offices start to slowly open back up, the post-pandemic world is changing its threat landscape once again, and that includes the likely inclusion of coronavirus phishing attempts. With the move to remote work, attackers switched up their tactics. Personal devices and home networks became hot targets. Organizations struggled with securing devices remotely, rolling out VPNs, and forming best practices for potentially sensitive work done outside the office environment. Plus, more workers used work devices for personal use which introduces an aspect of risk that many organizations perhaps weren't dealing with previously. Employees are now indeed being targeted with "back to the office" missives. One such e-mail claims to be an [EXTERNAL] e-mail notice from the CEO, welcoming people back to the office as they update their "business operations." The e-mail then contains a link for the user to "update your network credentials" in advance of returning to the office. Of course, this is a sham portal wherein the user has now given the cybercriminal their login information, permitting unfettered access to the company's network. This approach is often more effective where companies don't have regular COVID status updates going out by mail, so employees react to the executive's request to be ready to return to the office network environment. So SIM2K wants our clients to be aware of this potential scam and have employees know not to fall prey to this phishing attempt.

New Collaboration Tools

As businesses eye a return to the office, many are settling on a mixed approach to remote and in-office work. For those outside of the workplace, this creates challenges in re-creating serendipitous and ad-hoc interactions – the digital equivalent of a tap on a colleague's shoulder, or watercooler chat. With the launch of Slack Huddles, Slack hopes to lower the barrier to start conversations in its app with "audio-first" meetings reminiscent of Clubhouse, Discord and other voice-based tools. Slack Huddles provides a more casual and informal approach to meetings that video apps tend to lack. A Slack spokesman said "Just like e-mail is not a great means to base all of your internal communication on, the formats that we have for meetings – blocks of 30 minutes, everyone in the conference room, or a screen of little rectangles and video feeds of people's faces – that can't possibly be it." Slack users can start an audio meeting with colleagues in either channel conversations or with direct messages by clicking a "headphones" icon in the left-hand sidebar. Once started, participants can share their screen to discuss a shared document, for instance. It's also possible to start an audio chat room with external participants, Slack said.

What's Old is New Again

The 1990s called and want their browser suite back. Vivaldi, one of the boutique browsers that fight for market share against Google Chrome and Microsoft Edge, has turned to a strategy reminiscent of Netscape Navigator, the world's first dominant web browser. Vivaldi 4.0, which launched earlier this month, added an e-mail client, calendar, and RSS reader to the already-available browser, creating the 21st century version of Netscape Communicator, that was released in 1997. Vivaldi says it is going against the current mindset because "A growing movement of people worldwide is looking for reliable, functional alternatives to the tools offered by the tech giants. We are building Vivaldi to meet that need – and more – with an expanded set of integrated features that give you more control of your data and your workflow." We'll see!

PrintNightmare Vulnerability Opens Networks to Attack

The CERT Coordination Center (CERT/CC) has released a vulnerability note for a critical remote code execution vulnerability in the Windows Print spooler service, noting: “while Microsoft has released an update for CVE-2021-1675, it is important to realize that this update does not address the public exploits that also identify as CVE-2021-1675.” An attacker can exploit this vulnerability – nicknamed PrintNightmare – to take control of an affected system.

CISA encourages administrators to disable the Windows Print spooler service in Domain Controllers and systems that do not print. Additionally, administrators should employ the following best practice from Microsoft’s how-to guides, published January 11, 2021: “Due to the possibility for exposure, domain controllers and Active Directory admin systems need to have the Print spooler service disabled. The recommended way to do this is using a Group Policy Object.” It took Microsoft some time to finally issue an alert about the 0-day, and Bleepingcomputer reports that the company is even warning customers that it’s being actively exploited. The vulnerability allows attackers to use remote code execution, so that hackers could potentially install programs, modify data, and create new accounts with full admin rights.

Microsoft admits “the code that contains the vulnerability is in all versions of Windows,” but it’s not clear if it’s exploitable beyond server versions of Windows. The Print Spooler service runs by default on Windows, including on client versions of the OS, Domain Controllers, and many Windows Server instances, too. Microsoft recommends disabling the Windows Print Spooler service (if that’s an option for businesses), or disabling inbound remote printing through Group Policy until a patch is installed.

Vulnerabilities in the Windows Print Spooler service have been a headache for system administrators for years. The most infamous example was the Stuxnet virus. Stuxnet used multiple 0-day exploits, including a Windows Print Spooler flaw, to destroy several Iranian nuclear centrifuges more than a decade ago.

Microsoft has released the KB5004948 emergency security update to address the Windows Print Spooler PrintNightmare vulnerability on all editions of Windows 10 1607 and Windows Server 2016. “An update has now been released for all affected versions of Windows that are still in support,” Microsoft said in the Windows message center.

While Microsoft says these security updates address the PrintNightmare vulnerability, security researchers have discovered that the patch is incomplete and it can be bypassed to achieve both remote code execution and local privilege escalation with the official fix installed. It also appears that the rollout is causing additional unwanted issues among users.

Shortly after releasing update KB5004945, a small number of users began to report that their printer stopped working after applying the patch. Although this has been affecting mainly Zebra printers, the problem is also affecting other brands. Microsoft has acknowledged the problem, and it is working to provide a permanent fix in the coming days.

If that wasn’t enough, some users seemed to have tried to work around the patch by editing the default print settings using the Registry. However, after an investigation regarding the effectiveness of the update, Microsoft claims that the “security update is working as designed and is effective against the known printer spooling exploits and other public reports collectively being referred to as PrintNightmare.” The company also recommends that after applying the update to check the Registry to confirm the settings are set 0 (zero) to keep the device secure

To install the patch, regardless of 100% effectiveness, to get started, you’ll need to open the **Start** Menu, and then click on the **Settings** icon on the left side of your screen. From there, you’ll be taken to the Windows 10 settings app, where you need to click **Update & Security** followed by **Check for Updates**. Windows 10 will then begin checking for updates.

If you’re on the latest version of Windows, which covers the May 2021 Update (21H1) to the May 2020 Update (20H1), you’ll need to make sure you see KB5004945 listed in Windows Update to fix PrintNightmare. This is the automatic patch for Windows 10 Home, Pro, and other versions of Windows 10 that addresses the issue.

Let Windows 10 download the update and install it in the background. After a few minutes, you will be prompted to restart your computer with the Restart Now button. Once you restart, things will be fixed.

If you’re on an older version of Windows 10, (Windows 10 November 2019 Update, aka 19H2), then you’ll be seeing KB5004946 as the patch. For all other versions of Windows 10 (Windows 10 April 2018 Update, aka version 1803), you should be seeing KB5004949 as the patch in Windows Update. In all cases, your PC will install right away and will require a quick restart.

Other companies are rushing to fill the void in protection for PrintNightmare. 0Patch (0patch.com) claims to have micropatches available to address the shortcomings of Microsoft’s update. These micropatches will not impact any other security updates from Microsoft, only covers the initial attempt from Microsoft to fix this vulnerability.

Any malware attack shows the need for security and effective updates from your software vendors. Multi-factor Authentication can and will stop unauthorized users from accessing your network. After all, credentials for regular users can be just as good for an attacker in environments vulnerable to privilege escalation, and there is a market for this type of data, sustained by info-stealing activities. On some underground forums, a valid login and password pair for a Windows Remote Desktop server can go for as low as $3 and as high as $70. One of the largest marketplaces for Windows Remote Desktop logins had a collection of 1.3 million credentials, showing that selling them is a lucrative business. So if $3 can get into your network, it is worth the cost to add MFA for your company’s protection.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com