SIM2K
Adapting Technology to Your Business Needs

9•20
Information you can use

SIMformation

Office 365 Updates Over The Summer

Office 365 and Microsoft 365 subscribers should always have the latest version of Microsoft Office — currently Office 2019. They also get more frequent software updates than those who have purchased Office 2019 without a subscription, which means subscribers have access to the latest features, security patches and bug fixes. But it can be hard to keep track of the changes in each update and know when they're available. Following are summaries of the updates to Office 365/Microsoft 365 for Windows over the past few months:

Version 2008 (Build 13127.20296) – Release date: August 31, 2020

This build offers a variety of new features and includes several bug fixes. You can now pin folders from the Save dialog in Excel, Word and PowerPoint. Across the entire Office suite, you can switch among multiple panes using a tab on the right side of an app. (The tab only appears if you have two or more panes open.) In Teams, you can use a variety of Cortana voice skills, such as for meetings or collaboration. In Outlook, when you include a link in an email, the file name automatically replaces the URL.

Among the bugs fixed are one that caused crashes when replying to or composing new e-mail in Outlook, and another in Project in which project finish dates weren't getting updated for projects connected to SharePoint tasks lists.

Version 2007 (Build 13029.20460) – Release date: August 25, 2020

This build includes a variety of minor bug fixes, including for one in Excel that occurred when trying to save a file that contained a formula with the LET() function, another in Outlook that caused issues when navigating in compact views, and another for the entire Office suite in which a crash could occur when a document was closed while the Share pane was open.

Version 2007 (Build 13029.20344) – Release date: August 11, 2020

This build includes 13 security updates, including for Remote Code Execution Vulnerabilities for Excel, Access, and the entire Office suite, as well as Information Disclosure Vulnerabilities for Excel, Word, Outlook and the entire Office suite. This build also fixes several small bugs, including one that caused Outlook to fail to retrieve search suggestions, and another that caused devices to occasionally crash when retrieving personal information from Outlook.

Version 2007 (Build 13029.20308) – Release date: July 30, 2020

This build offers a variety of new features and squashes several bugs. You can now create pivot tables from datasets in Power BI within Excel, and also connect to, import, and refresh data from a PDF in Excel. In Outlook you can create polls with Quick Poll and quickly reopen items from previous sessions. PowerPoint and Word now let you auto-apply or recommend sensitivity labels. Teams gets a variety of changes, including simplified notification settings and turning off previews for your chat notifications.

Among the issues fixed are one that caused and error or hang in Excel when loading a workbook with multiple sheets in page break preview and another in Project in which the task selected in the assign resources dialog wasn't the same as the task selected in the task board view. A bug was fixed for the entire Office suite that caused a runtime message to show even though the transition to the full product is complete.

Version 2006 (Build 13001.20266) – Release date: June 30, 2020

This build offers a variety of new Office feature and squashes a number of bugs. Excel now supports OneDrive/SharePoint files with names and paths of up to 400 characters. Among other changes, PowerPoint has improved streaming video performance, Teams gets a simplified way to manage channel notification settings, and Outlook offers an option to disable @ mention suggestions when you're composing mail in Outlook.

Among the issues resolved are one that caused users of the Shared Calendar improvements to see calendar failures in Outlook, and another that wouldn't allow projects to be opened in the Project desktop client from Project Web App if the URL ended in .com.

Hopefully all Office 365 users have seen these improvements come through in their use of the various tools in this office suite. If you are an Office 365 client, and have questions about either determining if your Office 365 is up to date, or if you need assistance in applying updates, then please contact SIM2K for help.

Microsoft 365 Security Issue

Critical vulnerabilities in multi-factor authentication (MFA) in Cloud environments where WS-Trust is enabled could allow attackers to bypass the MFA challenge and directly access cloud applications such as Microsoft 365, which uses the WS-Trust protocol.

As a result of the way Microsoft 365 session login is designed, an attacker could gain full access to a target's account including their mail, files, contacts, data and more. At the same time though, these vulnerabilities could also be leveraged to gain access to other cloud services from Microsoft including production and development environments such as Azure and Visual Studio.

The vulnerability was discovered by researchers who tested several Identity Provider (IDP) solutions, identified those that were susceptible and resolved the security issues. Microsoft is aware that the WS-Trust protocol is "inherently insecure" and says that it will cease using this protocol in October and introduce a new security platform over the next year for those Cloud clients.

The researchers found that in some cases, an attacker can spoof their IP address to bypass MFA using a simple request header manipulation while in others altering the user-agent header caused the IDP to misidentify the protocol and believe it was using Modern Authentication. According to the researchers, in all cases Microsoft logs the connection as "Modern Authentication" due to the exploit pivoting from the legacy protocol to the modern one.

With more employees working from home during the pandemic, MFA has become a must-have security layer for Cloud applications. However, there are several ways to bypass this protocol. The first of these is **real-time phishing** in which an attacker steals a user's information by a technique called "challenge reflection" where users are prompted to fill in their MFA credentials at a phishing site where they are distributed to the attackers in real time.
Channel hacking is another method used to bypass MFA where a victim's phone or computer is hacked with malware. This malware can then use "man in the browser" spyware to capture the login information. Finally, a more scalable method of bypassing MFA leverages legacy protocols for attacks on cloud accounts. This **bypass method** can be easily automated and applied to credential dumps from the web or credentials obtained from phishing. This is the exploit that the researchers have uncovered that can impact Microsoft 365 users.

While MFA can provide an extra security layer to protect user accounts, using a physical security key can provide even greater protection for user credentials as a physical device is required to access their on-line accounts. Much like a flash drive, this device plugs into the PC's USB port and provides the credentials to validate the user.

SIM2K can assist you with establishing a security protocol to protect your employees and their Cloud-based work. Call us for more information.

Vulnerability Management for All

In the battle against cyber adversaries, IT security professionals like SIM2K are having to carefully balance competing objectives; protecting your business assets and processes while enabling legitimate business operations and initiatives. Maximizing both objectives is challenging given differing business environments our customers face. Unfortunately, some times sacrifices in cyber defenses and acceptable risk are made to facilitate business operations as companies believe vulnerability testing is only for "Fortune 500"-type companies.

This increases demand for security service providers to support their clients in assessing and managing cyber risks with greater effectiveness. Further, with cybercriminals initiating attacks spread over many targets, businesses need a partner that can deliver effective security services at scale for many clients across multiple attack vectors.

Managed Service Providers (MSPs) like SIM2K take on an important role in protecting enterprises across the board. There are many attributes to be taken into consideration by customers before choosing a managed services provider that offers effective Vulnerability Management (VM) technology. Cloud hosting has made it easier for VM companies to provide solutions through MSPs. It brings their solutions to bear quickly and easily. With customers increasingly requesting more proactive security measures to defend against the evolving cyber threats, MSPs are adopting more advanced solutions to better detect and anticipate the potential threats.

Additional benefits of security partnerships with MSPs:

- Bidirectional Cooperation: The relationship developed between a MSP and their customers is built over time. We have a broad knowledge of your business and needs. Partnering enables a VM technology vendor to bring their solutions to a pre-primed customer base as their MSP has "vouched" for them through the client/provider relationship.
- Time to Market: Many VM vendors chose to work through local MSPs rather than building a dedicated sales force, enabling them to bring their products to a customer faster as the MSPs can go directly to clients with a solution in hand rather than the VM taking time to conduct prospecting and pre-sale qualification to reach the marketplace.

Due to the rising incidents of advanced cyber-attacks, customers are increasingly looking beyond traditional security management and monitoring services toward more advanced detection and remediation capabilities. New security technologies are always on the horizon, and as MSPs are the client's "trusted advisor," partnering with leading VM as a service provider will enable rapid deployment of new technology and more satisfied clients. This is why SIM2K is constantly evaluating new opportunities in VM to find the best solutions for our customers for your company's IT security. Call us for more information on our vulnerability scanning capabilities and the partnerships we have fostered with leading security providers.

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.

Is TikTok a Danger?

In recent news retail giant Amazon sent a memo to employees telling them to delete the popular social media app TikTok from their phones. In the memo it stated that the app would pose a security risk without going into details. Later the memo was withdrawn without an explanation except that it was sent in error.

For those of us that can't tell one social media app from another, TikTok is one of the most popular ones and it was especially designed to allow users to upload short video's for others to like and share. Functionality, it has grown from a basic lip-sync app to host a wide variety of short video clips. It is predominantly popular among a younger audience. Most of the users are between 13 and 24 years old. In the first quarter of 2019, TikTok was the most downloaded app in the App Store, with over 33 million installs. TikTok is owned by a Chinese tech company called ByteDance.

Amazon's move wasn't the first time TikTok faced removal from a number of devices. India already banned TikTok. And the USA and Australia are also considering blocking the app. In fact, in December, the US Army banned TikTok from its phones, and in March, US senators proposed a bill that would block TikTok from all government devices.

The safety of using TikTok begins with TikTok being a Chinese product which does not help. A number of Chinese apps and software packages have been under investigation and were found to be "calling home". Now this does not automatically mean they are spying on you, but when you start your investigation with a negative expectation, you are inclined to see it as such. And gathering information about a client without their consent is wrong. The fact that TikTok is different in China itself, where it goes under the name Douyin, is another factor. But this could be explained away as well as China has a reputation of spying on its population. So maybe the foreign version is less intrusive than the domestic one. And some governments have their own reasons not to trust anything from Chinese origin or another agenda to boycott products originating from China.

Adding to the suspicion a Reddit user posted comments about the data found to be sent home when he reverse-engineered the app. One type of behavior that was confirmed by another source is that the app copies information from the clipboard. Which certainly is something that goes above and beyond what other social media apps do.

TikTok's main defense consists of the fact that most of their senior staff are outside of China. On their blog they also specified where their data are stored and that the data are not subject to Chinese law. "TikTok is led by an American CEO, with hundreds of employees and key leaders across safety, security, product, and public policy here in the US. We have never provided user data to the Chinese government, nor would we do so if asked."

Posting personal information on social media always poses a risk, but can be managed by common sense in what you post. But when the social media app itself is determined to mine your data it becomes a whole different story. There is no conclusive proof that this is true for TikTok, but some of the allegations are very serious and seem to be supported by facts and authoritative research. However, to be prudent, TikTok may not have a place on any company-owned device. Call us for more information on securing devices against third-party monitoring.

"Random Tid-Bytes"

Stalkerware Survey Has Interesting Results

The Online Creeping Survey was conducted by NortonLifeLock, and found that 46% of more than 2000 US respondents admitted to "stalking" an ex or current partner online "by checking in on them without their knowledge or consent." Twenty-nine percent of those surveyed admitted to checking a current or former partner's phone. Twenty-one percent admitted to looking through a partner's search history on one of their devices without permission. Nine percent admitted to creating a fake social media profile to check in on their partners. It would seem that online stalking is considered more acceptable when couched under the term "checking in." For perspective, if one were to swap the word "diary" for "phone," we don't think too many people would feel comfortable admitting, "Hey, I'm just 'checking in' on my girlfriend/wife's diary. No big deal." However, there is a distinction between consensual location-sharing apps and the more intrusive types of monitoring that stalkerware can provide. Many people who said they use apps like "Find my iPhone" to check up on a partner's location do it for their partner's safety if they are out jogging or bike riding, or if they are monitoring their teenagers whereabouts, as opposed to more nefarious location monitoring.

Malware Terms to Know

The "bad guys" continue to assault users, and their techniques vary constantly. In addition to ransomware and phishing attacks, here are some other ploys being used:

Pharming malware aka DNS changers/hijackers infect a victim's computer and stealthily make changes to the victim's hosts file. It helps to think of your computer's hosts file as a Rolodex of websites. As mentioned, the process of sending a domain name to a DNS server and translating that domain name into an IP address usually happens so quickly most of us don't even notice. "Usually" being the operative word here. To avoid any hang ups when loading a page, your computer stores domain name to IP address translations, cutting down the time it takes to load each website. With a malware-based pharming attack, the malware sneaks its way on to your computer (frequently via Trojan) then starts modifying your hosts file so that the domain name of a given website points to a malicious site. Some pharming malware, e.g., the Extenbro Trojan, will also block access to cybersecurity sites, preventing victims from downloading software to remove the DNS changer malware.

DNS poisoning aka DNS spoofing takes advantage of exploits in the software that controls DNS servers in order to hijack the servers and reroute web traffic. Typically, DNS poisoning goes after the companies that run and maintain the DNS servers that translate human-friendly domain names into computer ready IP addresses. As such, DNS poisoning has a much broader base of potential victims, numbering in the tens of thousands. That said, your home Internet router has a DNS cache that stores previous DNS lookups. Any device connected to your home network can refer to this cache when trying to connect to a website you or someone else on your network has visited before. Your router functions, after a fashion, as a small-scale DNS server and it too can be poisoned.

Make Windows 10 Work Faster

Want Windows 10 to run faster? Here are some hints on tweaks to your PC that will help improve the performance of Windows 10:

Change your power settings
If you're using Windows 10's "Power saver" plan, you're slowing down your PC. That plan reduces your PC's performance in order to save energy. (Even desktop PCs typically have a "Power saver" plan.) Changing your power plan from "Power saver" to "High performance" or "Balanced" will give you an instant performance boost. To do it, launch the Control Panel app, then select Hardware and Sound > Power Options. You'll typically see two options: "Balanced (recommended)" and "Power saver." To see the "High performance" setting, click the down arrow by "Show additional plans." To change your power setting, simply choose the one you want, then exit Control Panel. "High performance" gives you the most oomph, but uses the most power; "Balanced" finds a happy medium between power use and better performance; and "Power saver" does everything it can to give you as much battery life as possible. Desktop users have no reason to choose "Power saver," and even laptop users should consider the "Balanced" option when unplugged – and "High performance" when connected to a power source.

Disable programs that run on startup
One reason your Windows 10 PC may feel sluggish is that you've got too many programs running in the background – programs that you rarely or never use. Stop them from running, and your PC will run more smoothly. Start by launching the Task Manager: Press Ctrl-Shift-Esc, right-click the lower-right corner of your screen and select Task Manager, or type task manager into the Windows 10 search box and press Enter. If the Task Manager launches as a compact app with no tabs, click "More details" at the bottom of your screen. The Task Manager will then appear.

Then, click the Startup tab. You'll see a list of the programs and services that launch when you start Windows. Included on the list is each program's name as well as its publisher, whether it's enabled to run on startup, and its "Startup impact," which is how much it slows down Windows 10 when the system starts up. To stop a program or service from launching at startup, right-click it and select "Disable." This doesn't disable the program entirely; it only prevents it from launching at startup – you can always run the application after launch. Also, if you later decide you want it to launch at startup, you can just return to this area of the Task Manager, right-click the application and select "Enable."

Shut off Windows tips and tricks
As you use your Windows 10 PC, Windows keeps an eye on what you're doing and offers tips about things you might want to do with the operating system. Having Windows watching what you're doing and offering advice can also make your PC run more sluggishly. So if you want to speed things up, tell Windows to stop giving you advice. To do so, click the Start button, select the Settings icon and then go to System > Notifications & actions. Scroll down to the Notifications section and uncheck the box marked "Get tips, tricks, and suggestions as you use Windows."

Stop OneDrive from syncing
Microsoft's cloud-based OneDrive file storage, built into Windows 10, keeps files synced and up to date on all of your PCs. It's also a useful backup tool so that if your PC or its hard disk dies, you still have all your files intact, waiting for you to restore them. It does this by constantly syncing files between your PC and cloud storage – something that can also slow down your PC. That's why one way to speed up your PC is to stop the syncing. Before you turn it off permanently, though, you'll want to check whether it is actually slowing down your PC. To do so, right-click the OneDrive icon (it looks like a cloud) in the notification area on the right side of the taskbar, then click the More button at the bottom of the screen. From the popup screen that appears, click "Pause syncing" and select either 2 hours, 8 hours or 24 hours, depending upon how long you want it paused. During that time, gauge whether you're seeing a noticeable speed boost.

If so, and you decide you do indeed want to turn off syncing, right-click the OneDrive icon, and from the popup, select Settings > Account. Click "Unlink this PC," and then from the screen that appears, click "Unlink account." When you do that, you'll still be able to save your files to your local OneDrive folder, but it won't sync with the cloud.

Disable transparency
You can disable the transparency effects that Windows 10 uses for the Start menu, the Taskbar and the Action Center. It takes a surprising amount of work for Windows to create these transparency effects, and turning them off can make a difference in system performance. To do it, from Settings, choose Personalization > Colors, scroll down to "Transparency effects" and move the slider to Off.

These tips can help improve your PC's performance. For additional help, our Support Team has lots more ideas, so feel free to call SIM2K for more information.

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