SIM2K
Adapting Technology to Your Business Needs

10•22
Information you can use

SIMformation

New Attack Targets Exchange ... Again

Microsoft has confirmed the existence of two critical vulnerabilities in its Exchange application that have already compromised multiple servers and pose a serious risk to an estimated 220,000 more around the world.

The currently unpatched security flaws have been under active exploit since early August, when security firm GTSC discovered customer networks had been infected with malicious webshells and that the initial entry point was some sort of Exchange vulnerability. The mystery exploit looked almost identical to an Exchange zero-day from 2021 called ProxyShell, but the customers' servers had all been patched against the vulnerability, which is tracked as CVE-2021-34473. Eventually, the researchers discovered the unknown hackers were exploiting a new Exchange vulnerability.

"After successfully mastering the exploit, we recorded attacks to collect information and create a foothold in the victim's system," the researchers wrote in a post published on Wednesday. "The attack team also used various techniques to create backdoors on the affected system and perform lateral movements to other servers in the system."

Microsoft confirmed that the vulnerabilities were new and said it was scrambling to develop and release a patch. The new vulnerabilities are: CVE-2022-41040, a server-side request forgery vulnerability, and CVE-2022-41082, which allows remote code execution when PowerShell is accessible to the attacker.

"At this time, Microsoft is aware of limited targeted attacks using the two vulnerabilities to get into users' systems," members of the Microsoft Security Response Center team wrote. "In these attacks, CVE-2022-41040 can enable an authenticated attacker to remotely trigger CVE-2022-41082." Team members stressed that successful attacks require valid credentials for at least one email user on the server.

The vulnerability affects on-premises Exchange servers and, strictly speaking, not Microsoft's hosted Exchange service. The huge caveat is that many organizations using Microsoft's cloud offering choose an option that uses a mix of on-premises and cloud hardware. These hybrid environments are as vulnerable as standalone on-premises ones.

GTSC's post said the attackers are exploiting the zero-day to infect servers with webshells, a text interface that allows them to issue commands. These webshells contain simplified Chinese characters, leading the researchers to speculate the hackers are fluent in Chinese. Commands issued also bear the signature of the China Chopper, a webshell commonly used by Chinese-speaking threat actors, including several advanced persistent threat groups known to be backed by the People's Republic of China.

GTSC went on to say that the malware the threat actors eventually install emulates Microsoft's Exchange Web Service. It also makes a connection to an IP address which is hardcoded in the binary. An independent researcher said the address hosts a fake website with only a single user with one minute of login time and has been active only since August.

The malware then sends and receives data that's encrypted with an RC4 encryption key that's generated at runtime. The researcher went on to say that the backdoor malware appears to be novel, meaning this is the first time it has been used in the wild.

People running on-premises Exchange servers should take immediate action. Specifically, they should apply a blocking rule that prevents servers from accepting known attack patterns. Microsoft's advisory contains a host of other suggestions for detecting infections and preventing exploits until a patch is available.

But then a day later, Microsoft revised its mitigation measures for the newly disclosed and actively exploited zero-day flaws in Exchange Server after it was found that they could be trivially bypassed. The two vulnerabilities, tracked as CVE-2022-41040 and CVE-2022-41082, have been codenamed ProxyNotShell due to similarities to another set of flaws called ProxyShell, which the tech giant resolved last year. In-the-wild attacks abusing the shortcomings have chained the two flaws to gain remote code execution on compromised servers with elevated privileges, leading to the deployment of web shells.

So, once again we are faced with a 0-day vulnerability, with no effective patch available at the time of the infection. We said it last year, "you can't patch fast enough." No small and medium sized business should be running on-prem any more. The risks outweigh the reward. This is why SIM2K is constantly adding new partners in our security stack in an attempt to provide all clients the best possible protection against any such incursions. Obviously a zero-day infection is the worst possible scenario, but be assured SIM2K will respond to any issues as the "fix" is announced and actually works. Call us for more information.

Uber Hack

At the end of September, Uber employees discovered that huge swaths of their internal network had been accessed by someone who announced the feat on the company Slack channel. The intruder, who sent screenshots documenting the breach to The *New York Times* and security researchers, claimed to be 18 years old and was unusually forthcoming about how it occurred and just how far it reached.

It didn't take long for independent researchers to confirm *Times* coverage and conclude that the intruder likely gained initial access by contacting an Uber employee over WhatsApp. After successfully obtaining the employee's account password, the hacker tricked the employee into approving a push notification for multifactor authentication. The intruder then uncovered administrative credentials that gave access to some of Uber's crown-jewel network resources. Uber responded by shutting down parts of its internal network while it investigates the extent of the breach.

It's not clear precisely what data the hacker had access to or what other actions the hacker took. Uber stores an array of data on its users, so it's possible private addresses and the hourly comings and goings of hundreds of millions of people were accessed.

According to the NYT the hacker socially engineered an Uber employee after somehow discovering the employee's WhatsApp number. In direct messages, the intruder instructed the employee to log in to a fake Uber site, which quickly grabbed the entered credentials in real time and used them to log in to the genuine Uber site.

Uber had multifactor authentication in place in the form of an app that prompts the employee to push a button on a smartphone when logging in. To bypass this protection, the hacker repeatedly entered the credentials into the real site. The employee, apparently confused or fatigued, eventually pushed the button. With that the attacker was in.

This sort of MFA will protect users if their password is compromised through a database breach. But as has been demonstrated repeatedly, they are woefully inadequate at stopping phishing attacks. So far, the only forms of MFA that are phishing-resistant are those that comply with an industry standard known as FIDO2. It remains the MFA gold standard.

Many organizations and cultures continue to believe that their members are too smart to fall for phishing attacks. They like the convenience of authenticator apps as compared to FIDO2 forms of MFA, which require the possession of a phone or physical key. These types of breaches will remain a fact of life until this mindset changes.

After rifling around, the attacker discovered powershell scripts that an admin had stored that automated the process of logging in to various sensitive network enclaves. It remains unclear what other data the hacker had access to and whether the hacker copied or shared any of it with the world at large. Uber updated its disclosure page to say: "We have no evidence that the incident involved access to sensitive user data (like trip history)."

So even a large tech-centric company is vulnerable to these ploys. This is why SIM2K offers training so employees know signs of phishing and other breach strategies the "bad guys" use.

Trashed Server = $35 million Fine

Federal regulators accused Morgan Stanley on Tuesday of "astonishing" failures that led to the mishandling of sensitive data on some 15 million customers.

Morgan Stanley was slapped with a $35 million fine from the Securities and Exchange Commission for extensive failures to safeguard personal identifying information on its clients.

Since at least 2015 Morgan Stanley did not properly get rid of devices holding sensitive customer data, according to the settlement.

In one episode described by the SEC, Morgan Stanley hired a moving company – one that had "no experience or expertise" in data destruction – to decommission thousands of hard drives and servers holding customer data. That moving company later sold thousands of Morgan Stanley devices, some of which contained personal identifying information, to a third party, the SEC said.

Those devices were eventually resold on an internet auction site – without the removal of the sensitive data, according to the settlement. Morgan Stanley was able to recover some of those devices, which contained "thousands of pieces of unencrypted customer data," the SEC said.

"The firm has not recovered the vast majority of the devices," according to the settlement.

Morgan Stanley's "failures in this case are astonishing," the SEC's enforcement division said in a statement. "If not properly safeguarded, this sensitive information can end up in the wrong hands and have disastrous consequences for investors."

Beyond the servers and hard drivers, the SEC found that Morgan Stanley failed to safeguard customer data and properly dispose of consumer report information in other ways, including when the firm shut down local office and branch servers. The settlement said that a Morgan Stanley review found that 42 servers, all potentially containing unencrypted data and consumer report information, were "missing."

Morgan Stanley agreed to pay the fine without admitting or denying the findings in the settlement. In a statement, Morgan Stanley said it is pleased to have resolved this issue and expressed confidence that no sensitive data was exploited.

"We have previously notified applicable clients regarding these matters, which occurred several years ago, and have not detected any unauthorized access to, or misuse of, personal client information," Morgan Stanley said in the statement.

If you have old or redundant IT equipment gathering dust in your office, call SIM2K. We provide safe disposal of tech gear including destruction of old hard drives and recycling of servers, desktops and laptops as well as other peripherals. We will be glad to consult with you on proper decommissioning and then final disposal of technology.

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.

Personal Data At Risk ... Why?

If a traveler's phone, tablet or computer ever gets searched at an airport, American border authorities could add data from their device to a massive database that can be accessed by thousands of government officials. US Customs and Border Protection (CBP) leaders have admitted to lawmakers in a briefing that its officials are adding information to a database from as many as 10,000 devices every year, The Washington Post reports.

Further, 2,700 CBP officers can access the database without a warrant and without having to record the purpose of their search. These details were revealed in a letter Senator Ron Wyden wrote to CBP Commissioner Chris Magnus, where the lawmaker also said that CBP keeps any information it takes from people's devices for 15 years.

In the letter, Wyden urged the commissioner to update CBP's practices so that device searches at borders are focused on suspected criminals and security threats instead of allowing "indiscriminate rifling through Americans' private records without suspicion of a crime." Wyden said CBP takes sensitive information from people's devices, including text messages, call logs, contact lists and even photos and other private information in some cases.

While law enforcement agencies are typically required to secure a warrant if they want to access the contents of a phone or any other electronic device, border authorities are exempted from having to do the same. Wyden also pointed out that travelers searched at airports, seaports and border crossings aren't informed of their rights before their devices are searched. And if they refuse to unlock their electronics, authorities could confiscate and keep them for five days.

As The Post notes, a CBP official previously went on record to say that the agency's directive gives its officers the authority to scroll through any traveler's device in a "basic search." If they find any "reasonable suspicion" that a traveler is breaking the law or doing something that poses a threat to national security, they can run a more advanced search. That's when they can plug in the traveler's phone, tablet or PC to a device that copies their information, which is then stored in the Automated Targeting System database.

A CBP official said the agency only copies people's data when "absolutely necessary," but didn't deny that the agency's officers can access the database, though he even said that the number was bigger than what CBP officials told Wyden. Five percent of CBP's 60,000 personnel have access to the database, he said, which translates to 3,000 officers and not 2,700.

Two years ago, the Senator also called for an investigation into the CBP's use of commercially available location data to track people's phones without a warrant. CBP had admitted back then that it spent $500,000 to access a commercial database containing "location data mined from applications on millions of Americans' mobile phones."

Not to be too political, but "Big Brother" anyone?

"Random Tid-Bytes"

Digital Whiteboards

The scope of workplace collaboration tools available to teams today stretches far beyond anything employees might have imagined two and a half years ago. When work-from-home orders swept the globe in early 2020, most organizations were focused on ensuring they had viable video and chat platforms in place. Now, as a significant proportion of employees have decided to work outside of the office for at least part of the work week, tools that do more than just support workers' basic communication needs are becoming more sought after. One product that has seen an explosion in growth this year has been the digital whiteboard. Also known as visual collaboration platforms or shared canvas apps, these tools let hybrid teams collaborate visually via an online interface. Typically accessed via web browser, visual collaboration apps create persistent workspaces where team members can collaborate from any device, in real time or asynchronously. In addition to drawing and writing tools, the apps offer users the ability to add images, videos, diagrams, sticky notes, and other elements. Several platforms offer integrations with enterprise tools such as Slack, Trello, Jira, Dropbox, Google Drive, and Microsoft Teams. Vendors in this space expect that as employees use this tool, it will lead to multiple types of collaboration, such as content creation, project management, mind mapping, and design sprints, not just simple diagrams.

Windows 11 Adoption Lagging

Your network is mostly running Windows 10 and you aren't really sure when you'll deploy the year-old Windows 11 OS. If this sounds like you, congratulations – you sound like the majority of respondents to a survey on what businesses are planning to do with Windows 11. Slightly more than 89% reported that Windows 10 remains the key desktop operating system used in their network. The rest are using Windows 7 (3.92%); Windows 11 (3.43%), Windows 8.1 (.49%), macOS (.49%) or Linux (.49%). Notably, more than half (51.23%) of the respondents don't know when will roll out Windows 11. One of the reasons cited for not upgrading is the beefed up hardware requirements for Windows 11, meaning they must purchase new systems before they can roll out Windows 11. Many others see Windows 11 as equivalent to Windows Vista – an OS release to live through and wait until whatever comes next. On the "plus side" there are enhanced security features in Windows 11 like Smart App Control. This adds protection from malware (including new and emerging threats) by blocking applications that are malicious or untrusted, which do add some benefits to moving to W11. So while we now have a year of experience dealing with Windows 11, and a new update has just been released tackling some of the early issues with W11, there are still no compelling reasons to upgrade from Windows 10 at this time. However, if you are interested, or are getting new machines pre-loaded with Windows 11, call SIM2K for an evaluation of existing computers or help integrating the new W11 boxes into your network.

Windows Troubleshooting

As people use Windows 10 or 11 in their daily work, problems, issues, and outright errors will sometimes occur. Then, it may be necessary to engage in troubleshooting exercises to attempt to diagnose underlying causes. Sometimes such identification can lead to attempted fixes. Sometimes such attempts even succeed. Other times, fixes may not be available, which may necessitate working around problems and/or reporting those problems to Microsoft or enlisting the help of one of SIM2K's system engineers. All this said, a certain discipline to troubleshooting Windows is likely to help get through the process and get back to work with minimum disruption.

Three basic activities, each involving careful observation and some documentation, direct most troubleshooting efforts. This is the information that our Support Team will also want to know if you turn to SIM2K for help. Briefly described, these consist of:

1. Observing and describing symptoms: On Windows devices, some symptoms are entirely overt. They will often include error messages that you can look up to directly identify causes.

   Other symptoms may be more general, such as "system runs slowly," "takes forever to boot," "application takes forever to launch," "long network latencies," and so forth. These latter kinds of problems can be more vexing and time-consuming to fix, but may be amenable to specific troubleshooting tools.

2. Matching symptoms to potential causes: For observed symptoms, online research will usually help to correlate potential causes. For observed error messages, potential causes will often be identified explicitly. (Warning: such identifications don't always pan out, but they often do.) Keeping track of identifications can be important when matching symptoms to causes. That's because many symptoms of Windows trouble may have multiple potential causes, only one (or some) of which will be actual causes.

3. Attempting fixes or workarounds based on potential causes: When a potential cause is identified, further research may lead to recommended or documented fixes. Keeping track of what's been tried is important so that you don't repeat the same (or similar) potential fixes – especially those that don't do anything.

When troubleshooting leads to fix attempts (as it often will), it's prudent to make an image backup before applying such fixes – and make sure you have tools at hand to restore that backup from alternate boot media. Why? Because the worst-case outcome from an attempted fix is a PC that won't boot or run properly. By booting from recovery media and restoring the pre-fix image backup, you'll get back to where you started with minimum muss and fuss. If you are not comfortable with this step, then call in our Support Team.

In step 3, there will often be repeated trial-and-failure maneuvers before a fix or workaround is implemented, or you run out of options. Keep track of the time you invest in troubleshooting, so you will know when to consider short-circuiting the process.

There's a kind of "universal panacea" to Windows problems you should keep in mind when you start troubleshooting. Basically, it involves replacing all of the OS files for whatever version of Windows you're currently running using setup.exe from a matching Windows image. This takes 15 to 30 minutes and fixes the vast majority of issues that require troubleshooting in the first place.

If you find myself 30 or more minutes into a troubleshooting exercise, you might start thinking, "Maybe I should do an in-place upgrade." Any time past that is not time well-spent for you, so that's when you should call in our experts.

But if you wish to give it a go, try the following troubleshooting tools to diagnose and fix the problem without overwriting the operating system files.

For example, if you are getting the dreaded "blue screen of death" stating some exotic error code, Microsoft offers a free command line tool called the Microsoft Error Lookup Tool, a.k.a. "ERR," that can help you understand more about what error codes seek to communicate. That makes this tool worth downloading and keeping around. The latest version is always available at from the Microsoft Download Center.

Indeed, when an error code is available for a problem, using the tool is the best way to search for fixes and/or workarounds to address that problem. Searching on error codes (using Google, for example) is a decent strategy for investigating causes and fixes. Restricting that search to microsoft.com will sometimes help, but that will provide "official" strategies that might omit known, but less-than-perfect workarounds. Check the Microsoft path first, and if it provides no joy, move onto third-party sources and solutions.

If you can't pinpoint an error code for your current trouble, don't despair. Your next move should be to turn to the Windows troubleshooters. Type trouble into the Windows search tool in either Windows 10 or Windows 11, and you should be able to launch the Control Panel item entitled "Troubleshoot computer problems." You can use its categories – Programs, Hardware and Sound, Network and Internet, and System and Security, to drill down more deeply into a specific problem area.

For example, one common problem area is issues with Internet connections. Because internet access problems are something any Windows user can relate to, run the Internet Connections tool to see what it does. It launches the tool, prompts the user to click Next, then offers two options: 1. Troubleshoot my connection to the Internet and 2. Help me connect to a specific web page. Upon picking 1, the tool runs diagnostics, which will report potential issues if any are detected.

When it can, a troubleshooter will also attempt to fix problems it diagnoses, and it also reports whether such repair attempts succeed or fail. This makes troubleshooters good, all-around "fix-it" tools for all kinds of common Windows problems or issues.

Despite all troubleshooting efforts, including the aforementioned in-place repair install, in some cases Windows trouble simply can't be vanquished. As we mentioned, your time is too valuable to get hung up on a "deep dive" into Windows issues, so don't hesitate to involve our Support Team. That's what we do. But if the issues involve your personal home PC, hopefully these tips will help you get back to working quickly.

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