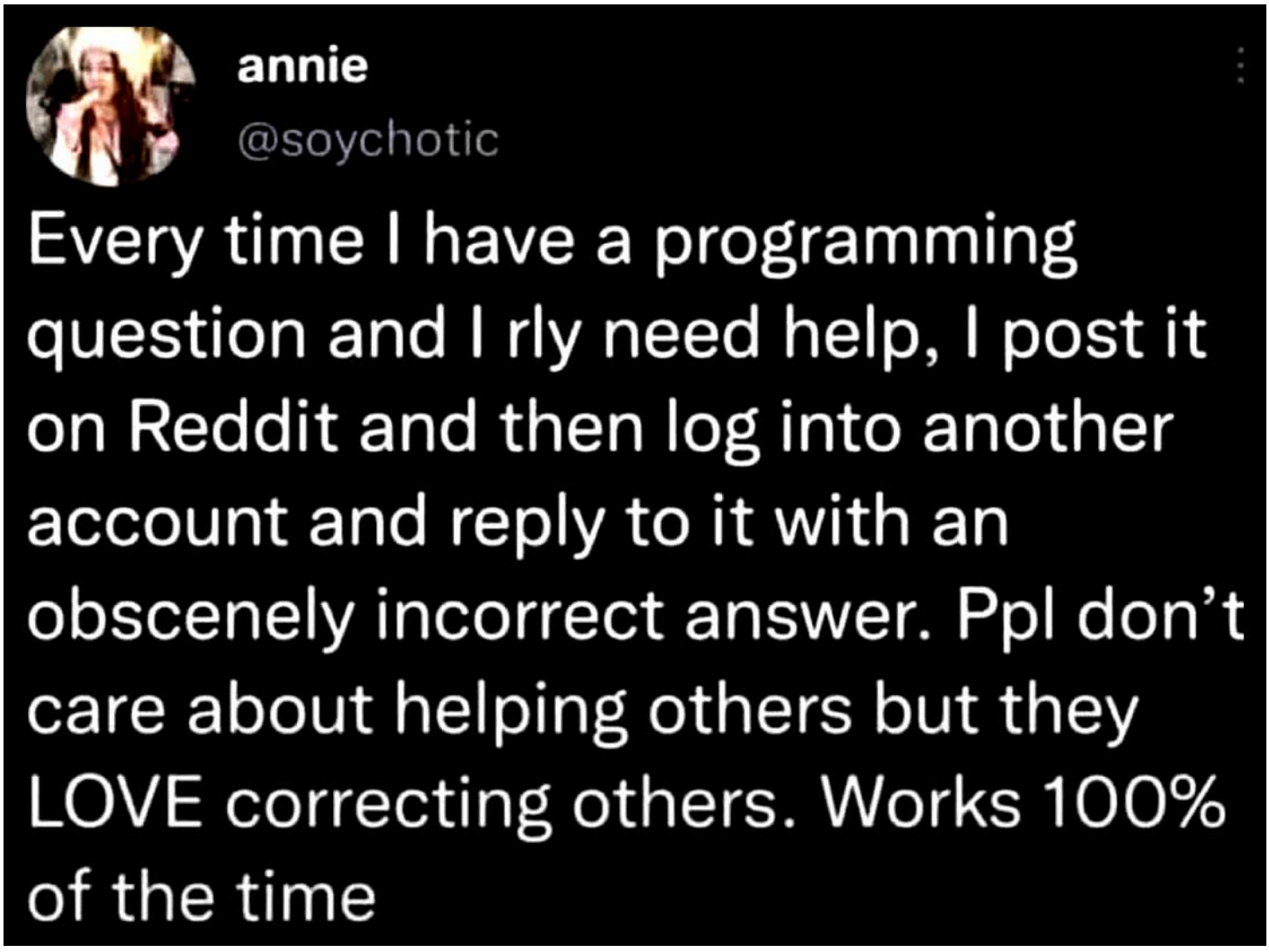
Security Now! #1036 - 07-29-25

Inside the SharePoint 0-day RCE

This week on Security Now!

• Brave randomizes its fingerprints. • The next Brave will block Microsoft Recall by default. • Clorox sues its IT provider for $380 million in damages. • 6-month Win10 ESU offers are beginning to appear. • Warfare has significantly become cyber. • Allianz Life loses control of 125 million customers' data. • The CIA's Acquisition Research Center website was hacked. • The Pentagon says the SharePoint RCE didn't get them. • A look at a DPRK "laptop farm" to impersonate Americans. • FIDO's passkey was NOT bypassed by a MITM after all. • Is our data safe anywhere? • The UK is trying to back-pedal out of the Apple ADP mess. • Meanwhile, the EU resumes its push for "Chat Control". • What happened after Microsoft fumbled the patch of a powerful Pwn2Own exploit?

How many times have we witnessed exactly this behavior?



Security News

Brave Browser Randomizes Fingerprints

Before I forget, as I did last week, I want to acknowledge all our listeners who wrote to let me know that the Brave web browser deliberately randomizes their browser fingerprints as reported by the EFF's excellent "Cover Your tracks" online testing facility. So for anyone who may have been unnerved and disturbed by the fact that neither uBlock Origin nor Privacy Badger, both which I was using on Firefox, were of any help in that regard, the Brave Browser looks like the right answer.

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	your browser has a randomized fingerprint

I wandered over to the Brave Browser site to look around. And when I saw that the browser natively supported vertical tabs, that cinched the deal for me. I've made the switch to Brave, so we'll see how that goes.

One thing I checked immediately was one of my enduring annoyances with Firefox, which is its ridiculous refusal to allow me to simply drag a URL from the browser's URL bar into a Windows Explorer folder or to the desktop. The day before, on Saturday, I needed to save some URLs so I was forced to copy the URL from Firefox, bring up Chrome, paste the URL into Chrome, then drag and drop the URL from Chrome into Explorer. I understand that this is a security measure, but please allow me to turn it off if it's interfering with my work flow, as it continually does. I've looked into disabling this nonsense and it's supposed to be possible to append the command-line option "--no-deelevate" to the shortcut that's used to launch Firefox. I've tried that to no avail, apparently because there's also some interaction with my desktop's UAC settings. Whatever the case, the bottom line is that the protection Firefox believes it's providing to me is not worth the hassle of not being able to simply drag and drop the URL of a page I'm viewing into a folder – and neither Chrome ***nor Brave*** similarly harass me.

The import of my Firefox settings went flawlessly, Brave let me turn off the unnecessary titlebar at the top of its window to save vertical space and to only have the browser's bookmarks display on a New Tab page. Both of which I appreciate. We'll see how it goes. So far, while I feel somewhat guilty about abandoning Firefox, and my support of it, I'm liking Brave a lot.

Brave to block Microsoft Recall by default

By pure coincidence, a piece of welcome news regarding the Brave browser surfaced last week. Anyone who might have been curious about Brave's stance on Microsoft Recall would have their curiosity satisfied by the headline which read: *"Brave blocks Microsoft Recall by default"*. They wrote:

> *Starting in version 1.81 for Windows users, Brave browser will block Microsoft Recall from automatically taking screenshots of your browsing activity.*

Microsoft first announced Recall in May 2024 and immediately drew fire from security and privacy advocates. Recall saved full-screen screenshots every few seconds and stored them in a local plaintext database, leaving it open for exploitation by anyone (including malware) who had access to the machine. The outcry caused Microsoft to hastily roll back the feature and re-work it significantly.

A year later, Recall is back, and Brave is ready for it. We will disable it by default for Windows 11+ users, with a toggle to turn it back on for users who really want Recall.

Microsoft has, to their credit, made several security and privacy-positive changes to Recall in response to concerns. Still, the feature is in preview, and Microsoft plans to roll it out more widely soon. What exactly the feature will look like when it's fully released to all Windows 11 users is still up in the air, but the initial tone-deaf announcement does not inspire confidence.

Given Brave's focus on privacy-maximizing defaults and what is at stake here (your entire browsing history), ***we have proactively disabled Recall for all Brave tabs****. We think it's vital that your browsing activity on Brave does not accidentally end up in a persistent database, which is especially ripe for abuse in highly-privacy-sensitive cases such as intimate partner violence.*

Microsoft has said that private browsing windows on browsers will not be saved as snapshots. We've extended that logic to apply to ***all*** *Brave browser windows. We tell the operating system that every Brave tab is 'private', so Recall never captures it. This is yet another example of how Brave engineers are able to quickly tweak Chromium's privacy functionality to make Brave safer for our users (inexhaustive list here). For more technical details, see the GitHub issue for this feature.*

Brave is the only major Web browser that disables Microsoft Recall by default in all tabs.

We were partly inspired by Signal's blocking of Recall. Given that Windows doesn't let non-browser apps granularly disable Recall, Signal cleverly uses the DRM flag on their app to disable all screenshots. This breaks Recall, but unfortunately also breaks the ability to take any screenshots, including by legitimate accessibility software like screen-readers. Brave's approach does not have this limitation since we're able to granularly disable just Recall; regular screenshotting will still work. While it's heartening that Microsoft recognizes that Web browsers are especially privacy-sensitive applications, we hope they offer the same granular ability to turn off Recall to all privacy-minded application developers.

We know that defaults matter. And I have little doubt that Brave browser users will be glad to know that regardless of anything else that might be going on, Microsoft Recall will not be able to snoop into their browser windows unless they explicitly choose to permit it. I have a feeling I'm going to like these Brave browser folks.

Clorox sues its IT provider for $380 million in damages.

In the wake of a whopping $380 million damages lawsuit being brought by the famous bleach maker, Cloxox against its IT provider Cognizant, it's foreseeable that future IT contracts will be adding a maximum damages clause to their boilerplate. Here's what Reuters News Service wrote under their headline "Clorox accuses IT provider in lawsuit of giving hackers employee passwords":

Bleach maker Clorox, said Tuesday that it has sued information technology provider Cognizant, over a devastating 2023 cyberattack, alleging that hackers gained access by simply asking the tech company's staff for its employees' passwords.
Clorox was one of several major companies hit in August 2023 by the hacking group dubbed Scattered Spider, which specializes in tricking IT help desks into handing over credentials and then using that access to lock them up for ransom.

The group is often described as unusually sophisticated and persistent, but in a case filed in California state court last Tuesday, Clorox said one of Scattered Spider's hackers was able to repeatedly steal employees' passwords simply by asking for them. According to a copy of the lawsuit reviewed by Reuters, "Cognizant was not duped by any elaborate ploy or sophisticated hacking techniques. The cybercriminal just called the Cognizant Service Desk, asked for credentials to access Clorox's network, and Cognizant handed the credentials right over."

In an emailed statement, Cognizant pushed back, saying it did not manage cybersecurity for Clorox and it was only hired for limited help desk services. They wrote: "Clorox has tried to blame us for these failures, but the reality is that Clorox hired Cognizant for a narrow scope of help desk services which Cognizant reasonably performed."

Three partial transcripts included in the lawsuit obtained by Reuters allege conversations between the hacker and Cognizant support staff in which the intruder asks to have passwords reset and the support staff complies without verifying who they are talking to, for example by quizzing them on their employee identification number or their manager's name.

"I don't have a password, so I can't connect," the hacker says in one call. The agent replies, "Oh, OK. OK. So let me provide the password to you OK?" Maxie Reynolds, a security expert who has specialized in social engineering and is not a party to the case said: "The apparent ease with which the hackers got what they wanted wasn't necessarily an indication that they weren't skilled. They just tried what typically works." She said the full transcripts were needed to offer a fair evaluation of what happened in 2023 but said that, "if all they had to do was call and ask straight out, that's not social engineering and it is negligence/non-fulfillment of duty."

The lawsuit said that the 2023 hack at Clorox caused $380 million in damages, about $50 million of which was tied to remedial costs and the rest attributable to Clorox's inability to ship products to retailers in the wake of the hack.

Clorox said the clean-up was hampered by other failures by Cognizant's staff, including failure to de-activate certain accounts or properly restore data.

It should be noted that Clorox asking for $380 million in compensatory damages doesn't mean that's what they're going to receive from a court or a jury trial. However, just looking at Reuter's reporting of this, I'm immediately skeptical of Cognizant's rebuttal. If, as they claim, they were only hired to perform limited help desk services, how was it that they had the ability to reset employee passwords at will? Their limited help desk services don't appear to have prevented that. And with the capability to arbitrarily reset Clorox employee passwords comes responsibility to do so responsibly.

What we clearly appear to have here is a case of outsourcing gone awry. Outsourcing is the new 21st century business model. It's the idea of hiring the services you need rather than growing them in house. The formal name for this is BPO – Business Process Outsourcing – It's now an

industry and I'm not a fan. I understand the promise of agility and scalability. Today's startups are essentially a small group of people with a bunch of contracts for the services they need. But what about a company like Clorox? Surely they could afford to operate and manage in-house IT services? And I'd wager they once did. I would bet that some pencil-necked C-suite executive got greedy and decided to "trim the fat" and demonstrate how they could shave half the cost of running IT in-house. And they may have reduced their IT operating overhead by half, right up until it cost them $380 million. It's easy to point fingers at some lame IT contractor, but it's probably also worth asking why Cognizant – who don't appear to have been quite cognisant – were ever given the opportunity to screw up so badly. In this business, you get what you pay for.

The Windows 10 Extended Security Updates (ESU) enrollment has started

We talked about this recently and last Tuesday Windows 10 end users will have begun seeing the notices we talked about before. Here's what Microsoft posted last Tuesday:

> *From modern security to faster performance and the latest features and experiences, Windows 11 is built to help you work, play and create with ease. With support for Windows 10 ending on Oct. 14, 2025, we're here to ensure your transition is smooth, secure and up to date.*
>
> *We understand that moving to a new PC can take time, and we're here to support you throughout the process. The Windows 10 Extended Security Updates (ESU) program is designed to keep your current Windows 10 PC protected after support ends—helping you stay secure during the transition.*
>
> *Starting today, individuals will begin to see an enrollment wizard through notifications and in Settings, making it simple to select the best option for you and enroll in ESU directly from your personal Windows 10 PC.*

I've seen no sign of it so far on my Win10 machines. Six days after that announcement I went poking around in Windows 10, looking for any sign of the ESU offer, but so far, nothing.

Warfare truly has gone cyber

The following story appeared last Friday in the online news publication RBC-Ukraine. While we might expect there to be some nationalistic bias in their reporting of the facts, the facts reported line up exactly with other sources. RBC-Ukraine's headline was: *"Cyber blast in Crimea. Ukrainian intelligence crashes Russian occupation servers"*. I wanted to share this because there's obviously no longer any question whether Russia and Ukraine are at war, and this story shows just how "cyber" today's modern warfare has become:

> *Cyber specialists from Ukraine's Defense Intelligence (HUR) have carried out a large-scale special operation targeting the occupation authorities in Crimea. According to a Ukrainian intelligence source speaking to RBC-Ukraine, the operation lasted several days. A powerful DDoS attack effectively paralyzed the information systems and network infrastructure in Crimea.*

That lines up with what we know of Ukraine's offensive cyber capabilities. They've demonstrated many times that they have the capability to launch and sustain significant DDoS attacks against their adversaries. The article continues:

> *While the Russian occupiers were scrambling to identify the cause of the government systems' failure, Ukraine's cyber experts infiltrated the electronic accounts of the leadership of the occupation administration in temporarily occupied Crimea. They gained access to the following digital resources:*
>
> - *The electronic document management system DIALOG,*
> - *The systems SED and Delo,*
> - *Accounting platforms 1C:Document Flow, Directum, and ATLAS.*
>
> *Over two days, 100 terabytes of documents belonging to the occupation authorities of the peninsula were downloaded. Among the files were "top secret" documents containing data on military facilities and logistics routes used to supply occupying forces in Crimea.*
>
> *A Ukrainian source said: "There's so much data extracted that we're about to learn a lot of explosive details about the operations and crimes of Russian occupiers in Ukrainian Crimea." After copying all valuable information, Ukraine's cyber specialists wiped all data stored on the servers of regional and district government bodies, ministries, and agencies of the occupation administration in Crimea.*
>
> *The successful Ukrainian hacker operation did not go unnoticed in Moscow. Russia's State Duma has already labeled it an element of hybrid warfare. Meanwhile, the so-called Ministry of Internal Policy, Information and Communications of Crimea stated that "technical specialists are taking all necessary steps to restore services. However, some services may remain unavailable to users." Notably, earlier this month, Ukraine's cyber specialists targeted the Russian company Gaskar Integration, one of the largest suppliers of drones for the Russian army. In June, Ukrainian hackers also attacked one of Siberia's largest internet providers, Orion Telecom. And earlier, RBC-Ukraine sources reported that Ukrainian intelligence cyber experts hacked into the online system of Russian Railways. As a result, the official website of Russian Railways went offline.*

I encountered another interesting piece of related news, which was that Russia has established free and open WiFi access zones so that their citizenry could continue to access the Internet where cellular services had been discontinued. It turns out that Russia has been forced to shut down large areas of cellphone service because Ukrainian drones were using those services for navigation.

It's clear that the battlefield is becoming more and more cyber. Not only is more cyber technology being employed for kinetic military operations, but all nations have become quite dependent upon the convenience created by today's networking for operational management. That fact that 100 terabytes of bureaucratic, operational and military data – some of it apparently "top secret" – were sitting on databases online and Internet-accessible would surprise no one today – but that doesn't make it any less irresponsible.

We've had fun through the years covering proof of concept stories where data was cleverly made to jump to and from air-gapped systems. Stuxnet is by far the most famous such

accomplishment. But the practical truth is, air-gapping is a huge pain in the butt to employ, specifically because it really works quite well. It may not be perfect, but it doesn't need to be. Even if it only drastically limits the bandwidth available for leakage due to operator errors, that would be a massive benefit. There's no way anyone is going to exfiltrate 100 terabytes of data from a camera that can see the blinking activity lights on a network router.

The personal data of 125 million Allianz Life customers – stolen.
While we're on the topic of being unable to keep the data we have inside our networks from getting out, TechCrunch carried the news of yet another major data breach – and just wait till you hear who did it and how it happened. TechCrunch wrote:

> *U.S. insurance giant Allianz Life has confirmed to TechCrunch that hackers stole the personal information of the "majority" of its customers, financial professionals, and employees during a mid-July data breach. When reached by TechCrunch, Allianz Life spokesperson Brett Weinberg confirmed the breach.*
>
> *Brett said: "On July 16, 2025 [13 days ago], a malicious threat actor gained access to a third-party, cloud-based CRM system used by Allianz Life. [Once again, bitten by outsourcing.] The threat actor was able to obtain personally identifiable data related to the majority of Allianz Life's customers, financial professionals, and select Allianz Life employees, using a social engineering technique."*
>
> *The company disclosed the data breach on Saturday in a legally required filing with Maine's attorney general, but did not immediately provide a number of how many Allianz Life customers are affected. According to the spokesperson, Allianz Life has 1.4 million customers while its parent company, Allianz, has more than 125 million customers worldwide.*
>
> *Allianz Life said it notified the FBI, and added it had "no evidence" that any other systems on its network were compromised. The insurance giant would not say if it had received any communication from the hackers, such as a ransom note. The company also would not attribute the breach to a hacking group.*
>
> *Allianz Life is the latest company in the past month to have been hacked during a wave of data breaches targeting the wider insurance industry, including Aflac, a major provider of supplementary health insurance. Security researchers at Google said in June that they were "aware of multiple intrusions" across the insurance sector attributed to **Scattered Spider**, a collective of hackers and techniques that rely on social engineering, such as deceptively calling and tricking helpdesks into granting them access to a company's network.*
>
> *Prior to targeting insurance companies, the Scattered Spider hackers were seen targeting the U.K. retail industry, as well as the aviation and transportation sectors, and are historically known for hacks targeting Silicon Valley technology giants. Per the Maine filing, Allianz plans to begin notifying affected individuals around August 1.*

So here we are again. As long as *"I forgot my password"* and *"I don't have my authenticator with me right now."* remain acceptable options we're just pretending to have security and we're **never** going to move past our current online impersonation problems. I mean, **really!**, what is the possible security benefit of even bothering with fancy time-based one-time token identity authentication if ***"oh, but I don't have it with me right now…"*** is acceptable??

Really! If you don't have it with you right now, that's just too bad. *"No login for you!"* Oh, does that inconvenience you? Good! That's what you asked for. That's what you signed up for. That's what you said you wanted. It's because you want to also significantly inconvenience any bad guys that it might be that you will also be inconvenienced if for whatever reason you might be unable to produce the exact thing that you want no bad guys to be able to produce. No one can have it both ways. You either have true security which might mean – and it would be on you – that you might be inadvertently locked out and unable to login when you're unable to meet the requirements you had previously arranged and agreed to.

Otherwise, we have the world we're actually living in today, where all we're allowed, the only thing available, is some feel-good security theatre using an authentication system which would most fairly be described as "optional". With optional authentication, not being able to produce the required magical 6-digits on demand simply means that it will be necessary to jump through some additional hoops to get yourself authenticated.

The problem is, bad guys are more than happy to jump through those same hoops. They wake up every morning in anticipation, wondering just how many hoops they're going to be able to jump through today? How many lazy fat Westerners' accounts are they going to hack into today?

But seriously... whenever I see one of those "I left my authenticator at home" links to click on underneath the authentication prompt I just shake my head. Why even bother with it if you don't actually need to use it? A cool and underappreciated feature of the SQRL system was that after its user became comfortable with the system, knew how it worked and had backed up their single global encrypted identity, they could enable a feature in the UI which requested every website they subsequently logged on to with SQRL to please immediately, completely and irrevocably disable every alternative logon solution and plant a flag in the account to prevent any human agent from ever overriding authentication no matter what anyone else ever says. That's what true security looks like, but the world is clearly still not yet ready to take their own security that seriously.

Even the CIA was recently hacked

The Washington Times last Thursday headline is "Hackers breach intelligence website used by CIA". I'm just going to share the intro of this, they wrote:

> *Unidentified hackers recently compromised a major intelligence website used by the CIA and other agencies to submit details of sensitive contracts, according to the National Reconnaissance Office, the spy satellite service that runs the site.*
>
> *The breach targeted proprietary intellectual property and personal information submitted on the Acquisition Research Center website in support of several innovative CIA spying programs. A National Reconnaissance Office spokesman told The Washington Times: "We can confirm that an incident involving our unclassified Acquisition Research Center website is currently being investigated by federal law enforcement. We do not comment on ongoing investigations." The extent of the breach is not fully known, but people familiar with the activity said hackers likely obtained information on key technologies for CIA operations.*

Other potential areas of compromise could include the Space Force, its efforts to build surveillance satellites and space weapons, and the Golden Dome missile defense program. Data from one highly sensitive program, Digital Hammer, was compromised, said people familiar with the hacking. Digital Hammer compiles cutting-edge technologies for human intelligence gathering, surveillance and counterintelligence operations. The program focuses on the threat of Chinese intelligence and information operations.

https://www.washingtontimes.com/news/2025/jul/24/major-intelligence-website-hacked-search-cia-spying-secrets/

The story continues at some length, so I put a link to the entire piece in the show notes for anyone who's interested in more. It's unclear whether we're going to obtain more reporting on this, given that it's the CIA. But my hunch, based upon the timing of the event and the nature of the breaches that are resulting from the exploitation of Microsoft's recent SharePoint disaster – which we'll be digging into when we get to today's main topic – I would not be surprised to learn that this CIA site, whose role and profile required it to be sharing files, might not have been another victim of that recent SharePoint 0-day remote code execution vulnerability.

The Pentagon says it was not "SharePoint" hacked

Speaking of the SharePoint hack, NextGov's headline last Thursday was *"Pentagon not impacted by Microsoft Sharepoint hack, tech chief says"*. They wrote:

The Department of Defense has not been ensnared by a broad intrusion into on-premises versions of Microsoft Sharepoint, its chief information officer said Thursday.

Katie Arrington said at the ATO and Cloud Security Summit Thursday in a stage interview: "As of right now, no, not that I'm aware of." Arrington said she's been doing daily calls with Microsoft while the department has been conducting forensics investigations since the 0-day vulnerability was publicly identified this past weekend.

Thus far, several federal agencies have been impacted, including the departments of Energy, Homeland Security and Education. And up to a dozen federal entities have been notified of possible compromise by the Cybersecurity and Infrastructure Security Agency, according to a source familiar. DHS issued a statement that its investigation into the hack remains ongoing but "there is no evidence of data exfiltration at DHS or any of its components at this time."

Arrington said the latest series of hacks — and attempted hacks — reiterate the constant threats posed by state actors to U.S. and defense systems. When 0-day vulnerabilities — which have not been previously uncovered and therefore give developers zero days to patch them — are found, cybersecurity professionals need to act immediately and apply those patches.

Arrington said: "Russia, China, Iran, North Korea, are they going to continue? Yes. Are they going to look for any hole that they can find? Yes. It's a 0-day the day you found out about it, a patch was made that same day. And how fast we deploy the patches, how fast we work as a unified body to, I say, turn the lights on an adversary when they do something, that's how fast resilience will be."

Okay. I have no idea what any of that double-speak mumbo-jumbo at the end was. But as we

know, patches, especially from Microsoft, often take much longer than, to quote Katie, "that same day." But what I really wonder, seeing what she said here, is whether Katie is aware that this entire quite serious mess was primarily created because Microsoft botched and fumbled the original Patch Tuesday patch release by, once again, only patching a symptom and not the underlying cause of the vulnerability? We'll be getting to that story shortly.

A DPRK Laptop Farm:

I had formed an image in my mind's eye, when I had previously discussed and described the so-called "laptop farms" which are commonly used to connect sanctioned North Korean IT workers to their domestic US jobs where they pretend to be Joe from Texas, despite having an odd accent and strange word usage. I had imagined something more glamorous than three metal wire racks containing about 30 assorted laptops with large fluorescent Post-It! notes used to identify which was which. I have a photo in the show notes of one such actual "laptop farm." I don't see any sign of a router or switch, so I wonder whether they're all sharing the same Wi-Fi?

A 50-year-old Arizona woman by the name of Christina Marie Chapman was recently sentenced to a term of eight and a half years in prison for this operation of an illegal North Korean laptop farm whose purpose was to help North Korean IT workers pass as US residents. Altogether, the workers managed to land more than 300 jobs at US companies and generated more than $17 million in revenue for the North Korean regime.

FIDO's passkeys system was NOT bypassed by an attacker-in-the-middle

Last week I shared the blog posting and forensic analysis by "Expel Security" describing a remote third-party man-in-the-middle attack on FIDO authentication using passkeys. Given Expel's description of the process, which amounted to a classic real-time website intercept and forwarding attack, the only way this could have been possible was if it was **not** necessary for the

passkey-equipped FIDO authenticator to communicate with the authenticating user's local desktop browser in real time. As I noted last week, the nature of this vulnerability is well understood. That's why I had incorporated a SQRL client-to-browser link using the Localhost IP to allow the user's browser to talk to the system's resident SQRL client.

Many of our on-the-ball listeners wrote to say that they were pretty sure that in FIDO's cross-device authentication model this client-to-browser link was not optional and that it must be present, created using Bluetooth. And they are 100% correct. FIDO explicitly prevents this attack and will not successfully authenticate without a local Bluetooth link between the user's web browser and their cross-device authenticator.

Given that, the presumably FIDO-based man-in-the-middle attack that Expel Security described having witnessed should not have been possible. It turns out that the attack was not possible and did not happen, at least not as they described.

Last Friday the 25th, they made another posting to their Threat Intelligence blog with the headline: *"An important update (and apology) on our PoisonSeed blog"* where they wrote:

> *On July 17, we published a blog post covering a recent incident we observed. On further review, we found our original findings are unsupported by the evidence. The original post described a new form of phishing attack that allowed an attacker to circumvent a FIDO passkey protected login. It stated that this attacker used cross-device authentication to successfully authenticate while not in close proximity to the authenticating client device.*
>
> *The evidence does show the targeted user's credentials (username and password) being phished and that the attacker successfully passed password authentication for the targeted user. It also shows the user received a QR code from the attacker. This QR code, when scanned by a mobile device, initiates a FIDO Cross-Device Authentication flow, which according to FIDO specification requires local proximity to the device which generated the QR code (the WebAuthn client). When properly implemented, but without proximity, the request will time out and fail.*
>
> *So, at the time of the original post, Expel believed the attacker successfully completed the authentication workflow, resulting in access to protected resources. After discussing these findings with the security community, we understand that this is not accurate. The Okta logs show the password factor passing successfully, but all subsequent MFA challenges failed and the attacker is never granted access to the requested resource.*

So that solves that mystery. I'm sure I also once knew that a Bluetooth link was required, and not optional, for FIDO cross-device authentication. And I'm very glad that's the case. But I got swept up in their report, which I assumed to be correct, and doubted what I knew. I suppose I also gave away the fact that I'm not a frequent user of FIDO passkeys cross-device authentication, since anyone who is likely deals with the need for that Bluetooth link any time they're in a new authentication environment.

Is our data safe anywhere?
Don't you start to get the feeling that our data is not safe anywhere? That no one can be trusted to keep anything we might disclose, and may need to disclose, safe online?

Here's another example we can add to the pile, and talk about sensitive personal data! TADTS are the initials of The Alcohol & Drug Testing Service. As their name suggests, they perform drug and alcohol testing, and they do so for multiple US states. Apparently not being in any great hurry – perhaps they were waiting for some statute of limitations to expire – the organization now admits that they were hacked and that those bad hackers stole the highly personal alcohol and drug testing data of 750,000 users. Yep. And even more gallingly, they waited a full year to disclose this. They became aware of the data breach last July 9th, 2024. The organization is only now notifying affected users but don't worry, they're offering free credit monitoring – to prevent the use of the highly confidential data they were entrusted with but turned out to be unable to protect.

I have no plans to unplug from the grid and live in a cave. My wife is a huge fan of indoor plumbing. But doesn't it really seem as though the rate at which we're losing this battle is accelerating?

Thank goodness there's a bit of good news!
The Financial Times' reporting is locked behind a paywall, but many other outlets are reporting on the Financial Times report. The Verge is one of those, writing:

> *The UK government is reportedly set to back down from its battle with Apple to obtain back door access to secure user data protected by the company's iCloud encryption. Victory hasn't come through the courts, or government figures changing their minds on privacy matters, but thanks to ongoing pressure from the US during the two countries' trade talks.*
>
> *Multiple unnamed UK officials told the Financial Times that the UK government is working on a way out. One of those sources said: "The Home Office is basically going to have to back down," adding that vice-president JD Vance was especially opposed to the UK's demand, which may violate the Cloud Act treaty between the two countries. <quote> "It's a big red line in the US — they don't want us messing with their tech companies."*
>
> *Another official echoed that, explaining that the UK wants to avoid pushing too hard for "anything that looks to the US vice-president like a free-speech issue." A third official said the UK had "its back against the wall," and wants a way out: "It's a problem of the Home Office's own making, and they're working on a way around it now".*

So this entire Apple Advanced Data Protection mess now appears destined to disappear. This is great news, and hopefully politicians and their governments won't put themselves and the rest of the world through many more of these no-win stand-off cycles. They need to realize that at least as regards privacy, they cannot simply demand anything they want. The laws of nature are not theirs to establish. There are problems, no doubt about it, arising from the abuse and illegal conduct enabled by the powerful privacy protections created by encryption technology. But

stripping privacy from everyone else cannot be the solution.

Denmark Reintroduces 'Chat Control'

However, we're not there yet since the publication *"EUToday"* posted the news under their headline: *"EU Reconsiders 'Chat Control' as Denmark Reintroduces Controversial Encryption Scanning Bill"* They write:

> *Known informally as 'Chat Control', the proposal has re-emerged under Denmark's EU Council Presidency, which began on July 1. Lawmakers are scheduled to debate the latest iteration of the bill on October 14, 2025.*

Let's hope the EU takes note of the egg the UK has ended up with on its face with reporting that the UK is backpeddling and trying to find a way out of the mess it's gotten itself into. The reporting continues:

> *Originally introduced in 2022 but repeatedly stalled due to political opposition, the legislation seeks to impose obligations on messaging platforms—such as WhatsApp, Signal, and Telegram—to scan user content for child sexual abuse material (CSAM). If adopted, the law could lead to widespread client-side scanning of messages before encryption, a measure that critics argue poses a serious threat to digital privacy and data protection.*

No one wants that to happen. But as I've noted here before, the solution I can see to this is to employ device-side local AI to examine what's being sent. It's creepy. And it's a mess because, for example, parents ought to be able to take photos of their own young children without the police being alerted. But if this must be done, do it device-side and don't mess with encryption backdoors. The article said:

> *The Danish Presidency has placed the proposal among its top legislative priorities. While no new text has been publicly released, Copenhagen has signalled its intention to find a compromise that balances law enforcement goals with legal and technical concerns raised by member states, civil society, and industry stakeholders.*

Good luck with that. No one wants to have Big Brother spying on them, even if Big Brother is inside their own phone.

> *The European Commission originally tabled the regulation in May 2022, aiming to bolster the detection and reporting of CSAM online. Despite its stated purpose, the proposal was criticised for its scope and method—particularly the inclusion of end-to-end encrypted services in the scanning regime.*
>
> *Attempts to pass the measure under previous presidencies, including Belgium and Poland, failed to secure a qualified majority in the Council. Belgium proposed a version in June 2024 that restricted scanning to shared media and URLs, contingent on user consent. Poland's February 2025 proposal classified scanning as a voluntary "preventive" action. Though regarded by some experts as an improvement, it too failed to gain traction.*

Denmark now assumes the role of broker, hoping to navigate between longstanding opposition from digital rights advocates and calls from several member states for stronger tools against online exploitation. The Danish Presidency's official programme states its intention to "strengthen the abilities to make use of the digital development for law enforcement when fighting serious crime, while also addressing the misuse of new technologies."

Criticism of the CSAM bill centres on concerns about weakening encryption. Client-side scanning—central to earlier drafts of the proposal—involves monitoring communications on a user's device before encryption takes place. This method is seen by experts as equivalent to surveillance and is considered by many to be incompatible with the principle of confidentiality of communications enshrined in EU law.

In 2023, the European Court of Human Rights issued a ruling that effectively prohibited states from requiring the weakening of secure encryption standards. This legal precedent, while not explicitly blocking the Chat Control proposal, adds a layer of complexity to its adoption and enforcement.

Digital rights organisations and privacy advocates have described the initiative as a disproportionate response to a serious problem. They argue that mandatory scanning mechanisms risk creating vulnerabilities that could be exploited by malicious actors and set a precedent for broader surveillance.

At present, the contents of Denmark's revised proposal remain undisclosed. Analysts suggest that the fate of the bill may hinge on Germany's position. The new federal government has not yet indicated whether it would support the measure, and without its backing, a qualified majority may remain out of reach. According to Patrick Breyer, former MEP for the German Pirate Party and a vocal opponent of the proposal, the Danish Presidency's success will depend heavily on its ability to secure German approval.

Even if the CSAM proposal were adopted in October, it would still need to proceed through trilogue negotiations with the European Parliament and Commission, where further amendments are likely.

The Chat Control bill is part of a wider series of initiatives by the EU aimed at giving law enforcement greater access to encrypted data. On June 24, 2025, the European Commission unveiled the first phase of its ProtectEU strategy, which proposes the development of decryption capabilities by 2030. The strategy is still at a conceptual stage but indicates the long-term policy direction of the European institutions.

While efforts to curb the spread of CSAM enjoy broad political support, the methods employed remain contentious. The question facing EU lawmakers is whether security objectives can be met without eroding the privacy rights of European citizens. As the debate resumes under the Danish Presidency, it is clear that any legislative outcome will need to reconcile fundamental rights with the imperatives of public safety—a task that has so far eluded consensus.

So the battle over the right to privacy and its inevitable abuse continues to rage. Governments are either going to give up on this or they're going to insist upon it. If it's insisted upon then at least the recent breakthroughs in local large language model image identification might provide the technology required. All that would be necessary would be for someone's phone to locally refuse to send an image, or to refuse to display an image without adult consent.

Listener Feedback

Mike Sander

Hello Steve, New subscriber. Long time listener. You have mentioned over the years how you are still using Win 7, and maybe Win 10. With Win 10 soon to go out of support, I wonder if you might consider discussing how you would (or not) use Win 10 after October. The tech press seems to view this as a "hair on fire" event. Perhaps I am numb to the risks. I have never had any antivirus beyond Defender. To the best of my knowledge I have never had a virus. I use FF pretty much exclusively. I really do not want to move to Win 11 for a variety of reasons. I am sure I do not need to enumerate. Your views on this topic might be of interest to others who listen. Regards, Mike

Windows 11 is extremely pretty. I recently set up dedicated Win11 machines at both of my development locations because I expected that I was going to need some time with Windows 11 before I'd be able to finalize the work on the DNS Benchmark. I assume that configuring Win11 for native whole-system encrypted DoH operation was going to drive the Benchmark crazy. But to my surprise the new DNS Benchmark code all worked perfectly under Windows 11. In any event, Windows 11 was so pretty that for a while I was a bit seduced by it. But that wore off. I've seen too many postings by people asking how they can go back to Windows 10 after making what they come to feel was the mistake of moving to 11. They report that their system feels much less responsive and snappy under 11 than it did under 10. Since I use Windows as my daily work platform, if I'm able to avoid losing any performance to rounded-corner animated zooming and fading Windows – lovely as they may be – and all the other stuff they've added for reasons that don't interest me, that's what I'm going to do.

So I'll be sticking with Windows 10 for the foreseeable future. And given that I'm still using Windows 7, whose support ended more than 10 years ago on January 13th, 2015, and that Windows 10 has an even stronger following today than Windows 7 did then, and that so many machines are compatibility-disabled to make the move to 11, I suspect that Windows 10 will refuse to die.

Having ridden the Windows 7 train I've seen that at some point in the probably distant future the browsers will start refusing to upgrade themselves any longer on Win10. But that only recently happened on Win7. And as we've often noted, the web browser is today's largest Internet-exposed attack surface by far – probably on a par with eMail clients.

My Win10 machines operate behind double layers of NAT routing and a pfSense firewall. And they have their own LAN segment to isolate them from the various IoT devices that are roaming around. And, like you, Mike, I've never had a virus or malware problem. It may be that my surfing is tame, and also that I never fail to treat the external Internet as a hostile foreign power. I'm never in too big a rush to bounce anything through a VirusTotal scan.

Given the maturity of Windows 10, which is significantly more than Windows 7, I cannot see any reason to feel pressured to move to Windows 11 only for the sake of an ongoing flow of security updates to repair all of the things they will be breaking in Win11. Having played with Windows 11 for a while, I readily understand its appeal. It's truly lovely looking. But I don't plan to move. And I'll be glad that Microsoft will continue leaving Windows 10 alone so that it will finally have the chance to settle down without them continually introducing new bugs that they then need to fix.

Dennis Borntrager

Does SpinRite 6.1 work on drives bigger than 2TB? I can't get it to do it.

Oh, yes. SpinRite v6.1 itself supports drives with up to 48 bits of sector addressing, which is the maximum sector count defined by the ATA drive standard. 48 bits worth of 512-byte sectors is more than 144 thousand terabytes. SpinRite will be able to access the entire surface of any drive connected directly to any motherboard. But I presume, Dennis, that you're connecting a larger drive to the system over USB. And that's the problem. The BIOSes of older motherboards were created before larger drives existed, and all versions of SpinRite so far have used the system's BIOS to provide USB drive support. SpinRite version 7 will be a native Windows application. So no more booting into DOS, the ability to operate on multiple drives at once, and much more. But I have a few other products to bring to market before I can get to work on SpinRite 7. In the meantime, if you can find a newer machine for SpinRite to run on, spinRite v6.1 will be able to see and operate on an entire large USB drive.

Rick LaBanca

In your second zero trust example, I thought all you need to do is hash the amount sold and give it to each other. A match means the same amount sold but the amount is not revealed.

Rick's question is a great example of why these zero knowledge proofs can be so tricky. The problem with his suggestion is that both parties could hash the various purchase quantities to obtain the direct hash equivalents of those quantities. Then, if either party were to reveal the hash of their quantity, the other party would see which of the hashes had been provided and they would immediately know the other's quantity. So in this case the hashes are just unique versions of the quantities.

The reason we needed to jump through all of those hoops with the locked boxes was to concoct an algorithm that would blind both parties to any knowledge other than whether or not they had purchased the same quantity. If not, they would still not know how many the other party had been permitted to purchase.

Lee MacKinnell

Hi Steve, On your comment about needing cheap biometrics for age verification, my smartphone in Australia cost me $100 Australian dollars. It is a Samsung Galaxy A15, it is a current model, released on 16 December 2023. It has a fingerprint sensor that I use with Bitwarden and passkeys. A flagship phone is not required. I bought this phone because it was affordable. Lee from Brisbane, Australia.

I appreciate Lee's note and I'm glad to know that low-end biometric-enabled smartphones are available. I checked the Internet and BestBuy was willing to offer a brand new Samsung A15 for $40 complete with free next-day shipping. The fact that it has a side-mounted biometric fingerprint sensor, multiple cameras, a nice high-res AMOLED screen, connectivity via WiFi, Bluetooth and NFC – and Android – means that it could almost certainly serve as a full-featured authenticator. And a price of $40 would be hard to beat for all that. It also offers biometric facial recognition. I know this because I was astonished by the price and purchased one for $40. And I'm still astonished by the fact that a state of the art Samsung Android smartphone can be had for $40.

One of the biggest problems with age verification is that it's difficult to see how it can be done without biometrics. Verifying someone's age only makes any sense at all if that verification can somehow be locked to their physical body. Any privacy requires that both the biometric lock and the real-time age verification with a remote site all be performed locally, without involving any sort of 3rd-party verifier in the loop. The web is littered with all of those "Login with Google" and "Login with Facebook" OAuth options, not only because they're magnanimously providing a genuinely useful service, but because every time anyone uses their service they learn who is logging into where.

What I'm getting at here is that I cannot see any way for age verification to be made available for no cost. The web itself can be used for no effective additional cost. Creating and using a username and password – even thousands of them thanks to password managers – is free. We support the Web by tolerating whatever advertisements and tracking may be going on.

Once upon a time, having websites encrypted with HTTPS using TLS connections was a high hurdle because TLS certificates were not free. So many websites refused, either on principle, lack of need, or due to economics, to keep using unencrypted HTTP. Let's Encrypt changed all that and successfully encrypted the Web. But as I noted recently, that was only possible because the only guarantee we're making with a web certificate is that the certificate matches the domain. And that need not cost anything.

I also noted that code signing certificates were not free and probably never can be because the issuer of the certificate – the Certificate Authority – needs to protect their own reputation and their granted ability to be a certificate signer by strongly verifying the identity of any organization that has them sign their code signing certificate. That's a far higher bar than automating the creation of certificates that match a domain name. And it's difficult to see how the economics of that will ever allow code signing certificates to be free.

In the case of age verification, I can see how the cost of age-to-person binding could be reduced by using existing consumer-facing government services such as the DMV, the post office, or any Notary service. But there's still the need for hardware. And although $40 for a Samsung smartphone is not nothing, it's a goal that would be within reach for most people. Verifiable, unspoofable age assertion should be free, but I cannot see how it ever can be.

Sable Cantus re: Project Hail Mary

Hi Steve, Long time listener, spinrite owner, and SoCal native here. I was listening to the show when you were thinking about the movie adaptation. I just wanted to share that I think we'll be in good hands with this movie. Last Saturday I attended San Diego Comic Con and went to the panel for Project Hail Mary. Andy was there with the directors, Ryan Gosling, and the same screen writer who wrote the Martian adaptation (Drew). They spoke about the production and story telling. We watched a few clips and the first 5 minutes of the movie.

Andy Weir said that Ryan brought more depth to Dr. Grace then was written in the book. Andy stated that every number you see on screen, every formula, even if it's blurred out, was Andy's work by hand. He made it clear that he spent hours verifying the science behind everything in the movie. I don't expect them to capture the entire journey of a huge book. I am impressed with what I saw at the panel. I don't think they are skimping out in any way. They did show the set for the "tube" and that alone showed me they aren't cutting corners :D

Keep up the good work, Steve. Live long, live well, and prosper. /Sable

Inside the SharePoint 0-day RCE

Today's podcast title leaves no room for misunderstanding: A remotely exploitable code execution vulnerability exists in all unpatched widely and long-used on-premises instances of Microsoft's SharePoint server. And more than 400 organizations have been attacked and hacked as a result of this flaw. Among the growing number of victims are several US federal and state agencies, universities, and hospital chains. Because a trio of Chinese APT groups appear to be behind the attacks we should perhaps not be surprised to learn that the US federal victims include the US Department of Homeland Security, the US National Nuclear Security Administration, and the US National Institutes of Health.

For those who are not tied into the enterprise world and may not be familiar with Microsoft's SharePoint, Microsoft says that SharePoint enjoys 200 million users. Here's how Wikipedia describes SharePoint:

> *SharePoint is a web application by Microsoft that is primarily used for building an intranet and managing and sharing files. Launched in 2001, it was initially bundled with Windows Server as Windows SharePoint Server, then renamed to Microsoft Office SharePoint Server, and then finally renamed to SharePoint. It can be used on premise or as a Microsoft 365 hosted service.*

This news was breaking while we were recording last week's podcast, but enough time has passed for the story to have taken shape. So I'm going to first share what WIRED wrote since it nicely places the story into context and provides some background. After that we'll examine what the security firms have found. WIRED wrote:

> *Hundreds of organizations around the world suffered data breaches, as an array of hackers rushed to exploit a recently discovered vulnerability in older versions of the Microsoft file-sharing tool known as SharePoint. The string of breaches adds to an already urgent and complex dynamic: Institutions that are longtime SharePoint users can face increased risk by continuing to use the service, just as Microsoft is winding down support for this platform in favor of newer cloud offerings.*
>
> *Microsoft said [last] Tuesday that, in addition to other actors, it has seen multiple China-linked hacking groups exploiting the flaw, which is specifically present in older versions of SharePoint that are self-hosted by organizations. It does not impact the newer, cloud-based version of SharePoint that Microsoft has been encouraging customers to adopt for many years.*
>
> *Bloomberg first reported on Wednesday that one of the victims is the United States National Nuclear Security Administration, which oversees and maintains US nuclear weapons.*
>
> *"On-premises" or self-managed SharePoint servers are a popular target for hackers, because organizations often set them up such that they are exposed to the open Internet and then forget about them or don't want to allocate budget to replace them. Even if fixes are available, the owner may neglect to apply them. That's not the case, though, with the bug that sparked this week's wave of attacks. While it relates to a previous SharePoint vulnerability discovered at the Pwn2Own hacking competition in Berlin in May, the patch that Microsoft released earlier this month was itself flawed, meaning even organizations that did their security diligence were caught out. Microsoft scrambled this week to release a fix for the fix, or what the company called "more robust protections" in its security alert.*

This really shouldn't surprise us. We've covered in the past how Microsoft's current incarnation of security updates appears to focused upon implementing a quick fix for the symptoms rather than addressing underlying systemic weaknesses. I don't know that's what happened in this instance, but if it quacks like a duck. WIRED continued:

> *A Microsoft spokesperson write in an emailed statement. "At Microsoft, our commitment—anchored in the Secure Future Initiative—is to meet customers where they are. That means supporting organizations across the full spectrum of cloud adoption, including those managing on-premises systems."*

Wow. Talk about writing a statement that says nothing. WIRED continues:

> *Microsoft still supports SharePoint Server versions 2016 and 2019 with security updates and other fixes, but both will reach what Microsoft calls "End of Support" on July 14, 2026.*
>
> *SharePoint Server 2013 and earlier have already reached end of life and receive only the most critical security updates through a paid service called "SharePoint Server Subscription Edition." As a result, all SharePoint server versions are increasingly part of a digital backwater where the convenience of continuing to run the software comes with significant risk and potential exposure for users—particularly when SharePoint servers sit exposed on the internet.*
>
> *Jake Williams, a longtime incident responder who is vice president of research and development at Hunter Strategy said: "Years ago, Microsoft positioned SharePoint as a more secure replacement for old school Windows file-sharing tools, so that's why organizations like government agencies invested in setting up those servers. And now they run at no additional cost compared to a Microsoft 365 subscription in the cloud that requires continuous payment. So Microsoft tries to nudge the holdouts by charging for extended support. But if you are exposing a SharePoint server to the Internet, I would emphasize that you also have to budget for incident response, because that server will eventually get popped."*
>
> *The United States Cybersecurity and Infrastructure Security Agency said in guidance about the vulnerability, Tuesday, that "CISA recommends disconnecting public-facing versions of SharePoint Server that have reached their end-of-life (EOL) or end-of-service (EOS). For example, SharePoint Server 2013 and earlier versions are end-of-life and should be discontinued if still in use."*

The problem is, it's working and it's been paid for. So when budgets are tight – and when are they not? – going through all of the hassle of switching to a paid Microsoft cloud-based service, and then needing to continue paying for it, can be a difficult sell to upper management.

As I've observed here recently, the entire model that's evolved across our industry, of selling online software systems that are later found to have critical vulnerabilities and expecting their users to suddenly take proactive responsibility – or even be aware that there's a problem that needs their attention, is inherently impractical and is badly broken in practice. WIRED's author apparently agrees with this, writing:

> *The ubiquity of Microsoft's Windows operating system around the world has led to other situations in which a long goodbye has created security issues for holdout users—and other organizations or individuals with connections to a vulnerable entity. Microsoft struggled to deal with the long tail of users on extremely popular Windows editions including Windows XP and*

Windows 7.

And now, of course, we're about to repeat this entire drama with Windows 10. WIRED wrote:

But legacy software is a challenge for any software or digital infrastructure provider. Earlier this year, for example, Oracle reportedly notified some customers about a breach after attackers compromised a "legacy environment" that had been largely retired in 2017.

The challenge with a service like SharePoint is that it often acts as an ancillary tool without ever being the center of attention.

Bob Huber, chief security officer at the cybersecurity company Tenable says: "For on-premises software like SharePoint, which is deeply integrated into the Microsoft identity stack, there are multiple points of exposure that need to be continuously monitored in order to know, expose, and close critical gaps."

When asked about the alleged breach at the National Nuclear Security Administration, the Department of Energy emphasized that the incident did not impact sensitive or classified data. A DOE spokesperson told WIRED in a statement: "On Friday, July 18, the exploitation of a Microsoft SharePoint 0-day vulnerability began affecting the Department of Energy, including the NNSA. The Department was minimally impacted due to its widespread use of the Microsoft M365 cloud and very capable cybersecurity systems. A very small number of systems were impacted. NNSA is taking the appropriate action to mitigate risk and transition to other offerings as appropriate."

Microsoft did not immediately return WIRED's requests for comment about the process of sunsetting SharePoint Server. The company wrote in a blog post on Tuesday that customers should keep supported versions of SharePoint Server updated with the latest patches and turn on Microsoft's "Antimalware Scan Interface" as well as Microsoft Defender Antivirus.

Unfortunately, as we saw, Microsoft fumbled and botched the security patch in this instance.

During May's Pwn2Own competition, which we covered at the time since it was the first time Pwn2Own had been held in Berlin, having moved from Toronto, a researcher with cybersecurity arm of Viettel, a telecom firm run by Vietnam's military, identified, a SharePoint bug dubbed "ToolShell" and demonstrated a way to exploit it. That discovery won the researcher an award of $100,000.

But here's where the plot thickens: Exploits discovered by security researchers remain explicitly secret. We only learn that there **is** a flaw and of its general nature, and nothing more. As part of the researcher's agreement, they confidentially provide all required information to Trend Micro's Zero-Day Initiative which then, in turn, forwards that information to the affected software vendor. The publication, The Register, theorizes that the exploit may have leaked from Microsoft. They wrote:

Less than two months later, on July 8, Microsoft disclosed the two CVEs – CVE-2025-49704, which allows unauthenticated remote code execution, and CVE-2025-49706, a spoofing bug – and released software updates intended to patch the flaws. But mass exploitation had already started the day before, on July 7.

Dustin Childs, head of threat awareness at Trend Micro's Zero Day Initiative (ZDI) said: "Sixty days to fix isn't a bad timeline for a bug that stays private and stays under coordinated disclosure rules. What is bad: is that a leak happened."

Patch Tuesday happens the second Tuesday of every month – in July, that was the 8th. But two weeks before then, Microsoft provides early access to some security vendors via the Microsoft Active Protections Program (MAPP).

These vendors are required to sign a non-disclosure agreement about the soon-to-be-disclosed bugs, and Microsoft gives them early access to the vulnerability information so that they can provide updated protections to customers faster.

Childs said: "The first MAPP drop occurs at what we call r minus 14, which is two weeks ahead of the [Patch Tuesday] release. In this case that was June 24. Then, on July 7, we started to see attacks. July 8, the patches were out and were almost immediately bypassed."

ZDI, along with other security providers, poked holes in the initial patches and determined that the authentication bypass piece was too narrow, and attackers could easily bypass this fix. In fact, anyone who received the early MAPP information about the CVEs and software updates would be able to tell that this is an easy way to get past it.

On July 18, Eye Security first sounded the alarm on "large-scale exploitation of a new SharePoint remote code execution (RCE) vulnerability chain in the wild." And a day later, Microsoft warned SharePoint server users that three on-prem versions of the product included a zero-day flaw that was under attack – and that its own failure to completely patch the holes was to blame.

But wait, there's more: Shodan shows that around 8,000 SharePoint servers in use by auditors, banks, healthcare companies, major industrial firms and U.S. state, federal and international government bodies. In other words, it's a mess. The 8,000 figure might be conservative because The Shadowserver Foundation, which scans the internet for potential digital vulnerabilities, put the number at a little more than 9,000, cautioning that ***that*** figure is a minimum, meaning that they were able to confirm 9,000 and that there are likely more. The Shadowserver Foundation said most of those affected were in the United States and Germany.

The final thing I want to share is some of the very interesting reporting by the researchers at Eye Security who were first to discover and report that attacks had gone viral. Remember that the first known instance of exploitation occurred on the day before the July 8th patch Tuesday which was exactly three weeks ago, today. The Eye Security researchers wrote:

On the evening of July 18, 2025, Eye Security was the first to identify large-scale exploitation of a new SharePoint remote code execution (RCE) vulnerability chain in the wild. Demonstrated just days before on X, this exploit is being used to compromise on-premise SharePoint Servers across the world. The new chain we uncover in this blog, was later named CVE-2025-53770 and CVE-2025-53771 by Microsoft.

Before this vulnerability was widely known last Friday, our team scanned over 23,000 SharePoint servers worldwide. In total, we discovered more than 400 systems actively compromised during four confirmed waves of attack:

- *The initial attack wave, 17th of July at 12:51 UTC from 96.9.125.147 (probably testing)*
- *Attack wave #1, 18th of July at 18:06 UTC from 107.191.58.76 (widely successful)*
- *Attack wave #2, 19th of July at 07:28 UTC from 104.238.159.149*
- *Then, multiple waves on and after the 21st of July after a public proof-of-concept exploit script was released on Github (multiple variants available).*

Remember that all of those attacks were effective against both unpatched -or- then fully patched SharePoint servers. So in this instance, it was Microsoft's significant fumble of the initial patches that were readily bypassed because they were merely cosmetic symptom-covering patches of the sort we've seen before. There are postings on the 'Net by people who "diff'ed" Microsoft's patch Tuesday updates to locate the flaw, then wrote code to side-step Microsoft's ineffective changes.

Note, also, that Microsoft's updated patches which do now actually resolve the problem only cover SharePoint Server 2016 and 2019. SharePoint Server 2010 and 2013 remain vulnerable with no patch expected. They must be either isolated from the public Internet or shut down.

So what, exactly, did the Eye Security guys see that led them to this? They explained:

Early in the evening, our 24/7 detection team received an alert from one of our CrowdStrike Falcon EDR deployment at a specific customer. The alert flagged a suspicious process chain on a legacy SharePoint on-prem server, tied to a recently uploaded malicious .aspx file.

At first glance, it looked familiar. A classic web shell, obfuscated code in a custom path, designed to allow remote command execution via HTTP. We've seen many of these before. What made this one stand out, however, was how it got there.

Our first hypothesis was mundane but plausible: a brute-force or credential-stuffing attack on a federated Active Directory identity, followed by an authenticated upload or a remote code attempt using valid credentials. The affected SharePoint server was exposed to the internet and tied into Azure AD using a hybrid ADFS. That stack, when misconfigured or outdated, can be a dangerous combination.

It all seemed to confirm the theory: credentials compromised → shell dropped → persistence achieved.

But examining the IIS logs more closely, we noticed that the Referer was set to /_layouts/SignOut.aspx . That's odd. How can that be an authenticated request, just after the user has logged out? Something didn't add up.

We found no successful authentications in ADFS logs, or the logging was at least insufficient…
Malicious IIS logs did not contain a value in the cs-username column…
A POST request to /_layouts/15/ToolPane.aspx seemed rather specific…
Referer set so /_layouts/SignOut.aspx cannot be authenticated, right?…

We began to develop a feeling that credentials were never used. So how could the attacker write files to the server, without authenticating at all? That's when we realized we were no longer dealing with a simple credential-based intrusion. This wasn't a bruteforce or phishing scenario. This was zero-day territory.

After some digging, we learned that three days earlier, the offensive security team from Code

White GmbH demonstrated they could reproduce an unauthenticated RCE exploit chain in SharePoint, a combination of two bugs originally presented at Pwn2Own Berlin earlier this year in May. Those bugs were still present in the patched SharePoint Server. They dubbed the chain ToolShell.

What we discovered on the 18th was not a credential issue. We had stumbled upon a weaponized Pwn2Own exploit already being used in the wild.

When our team began reviewing the impacted systems, we expected to find the usual suspects: standard web shells designed for command execution, file uploads, or lateral movement. Instead, what we discovered was more subtle, and arguably more dangerous: a stealthy spinstall0.aspx file whose sole purpose was to extract and leak cryptographic secrets from the SharePoint server using a simple GET request.

This wasn't your typical webshell. There were no interactive commands, reverse shells, or command-and-control logic. Instead, the page invoked internal .NET methods to read the SharePoint server's MachineKey configuration, including the ValidationKey. These keys are essential for generating valid __VIEWSTATE payloads, and gaining access to them effectively turns any authenticated SharePoint request into a remote code execution opportunity.

Then it all clicked together. Once the MachineKey confirmation, including the ValidationKey had been obtained, future payloads can embed any malicious commands and would be accepted by the server as trusted input, completing the RCE chain without requiring any credentials. This mirrors the earlier SharePoint design weakness exploited four years ago in 2021, but it's now been packaged into a modern 0-day chain with automatic shell drop, full persistence, and zero authentication.

More than 24 hours after we published our initial findings and reached out to affected vendors, including Microsoft, the Microsoft Security Response Center (MSRC) issued an official advisory and assigned vulnerability identifiers. On their page, Microsoft confirmed active exploitation in the wild and acknowledged the severity of the issue.

They make one final crucial point, due to the fact that this is a MachineKey exfiltration attack:

The attack we've observed specifically targets the exfiltration of SharePoint server ASP.NET machine keys. These keys can be used to facilitate further attacks, even at a later date. It is ***critical*** *that affected servers rotate SharePoint server ASP.NET machine keys and restart IIS on all SharePoint servers. Patching alone is not enough. If you are not targeted, or you are unsure, we also advise teams to rotate their Machine Keys just to be sure. It has no system impact, only that IIS is offline for some seconds while restarting services.*

We don't know how many systems, enterprises, organizations and networks have been compromised as a result of Microsoft's botched patches for the original Pwn2Own 0-day. But that number lies somewhere between the 400 that have been confirmed and the 9,000 that were vulnerable. And the attackers were aggressive and automated. This is a great deal of damage and the ransomware demands have already begun. As an industry, we need to do better. We need to change the model.

This has been an important high profile incident that individual reports have now been published by Broadcom Symantec, CISA, Cisco Talos, Censys, Check Point, CrowdStrike, Eye Security, Logpoint, Microsoft, Orange, Palo Alto Networks, Qualys, SentinelOne, Tenable, Trend Micro, Varonis.

In other words, pretty much everyone in the business.