Security Now! #1047 - 10-14-25

RediShell's CVSS 10.0

This week on Security Now!

• The EU aborted their Chat Control vote knowing it would fail. • Salesforce says it's not going to pay; customer data is released. • Hackers claim Discord breach netted 70,000 government IDs. • Microsoft to move Github to Azure. What could possibly go wrong. • New California law allows universal data sharing opt-out. • OpenAI reports that it's blocking foreign abuse. Who cares. • IE Mode refuses to die, so Microsoft is burying it deeper. • The massive mess created by Texas legislation SB2420. • The BreachForums website gets a makeover. • 100,000 strong global botnet attacking U.S. RDP services. • UI experts weigh in on Apple's iOS 26 user-interface. • 330,000 publicly exposed REDIS servers are RCE-vulnerable.

To prevent dementia patients from leaving the hospital, the code required to access the elevator is embedded into the notice:

Security News

The EU scraps Chat Control without voting

The much anticipated vote among EU member countries, originally slated for today, October 14th, was called off once it became clear that the vote for the adoption of the controversial measure would fail. Thankfully, Germany made up their mind, signaling a firm "no". I learned of this from a blurb on the "Risky Business" newsletter, which offer some addition detail, writing:

> *The European Union has scrapped the vote on Chat Control, proposed legislation that would have mandated tech companies to break their encryption to scan content for child abuse materials. The project was supposed to be put to a vote on Tuesday, October 14, during a meeting of interior ministers of EU member states.*
>
> *Denmark, which currently holds the EU presidency and was backing the legislation, scrapped the vote, according to reports on Austrian and German media. Danish officials scrapped the vote after failing to gather the necessary votes to pass the legislation and advance it to the EU Parliament. Only 12 of the bloc's 27 members publicly backed the proposal, with nine against, and the rest undecided. The final blow to Chat Control came over the past two weeks when both the Netherlands and Germany publicly opposed it. Germany's Justice Minister, Dr. Stefanie Hubig, went out of her way to describe Chat Control as a "taboo for the rule of law," arguing that the fight against child pornography does not justify removing everyone's right to privacy.*
>
> *The law has seen the usual mass opposition from privacy groups, such as the EFF, but also from the tech sector, too, with over 40 major EU tech companies signing an open letter to EU officials. Signatories described Chat Control as a "blessing for US and Chinese companies," since EU users will migrate to products that respect their privacy and ignore Chat Control.*
>
> *The Chat Control opposition also received major help from a Danish programmer, whose Fight Chat Control website allowed Europeans to mass-mail their representatives and urge them to vote against. According to a Politico Europe report, the website had driven so much traffic that it "broke" the inboxes of EU members of Parliament over the past weeks.*

It's one thing to be living within a government that declares itself to be a democracy. But it's truly wonderful to see a movement where the voices, opinions and feelings of that democracy's subject citizens can be and are heard.

I checked out that open letter to the EU Parliament that was signed by 40 major European Union companies. Since this is one of the major issues of our time, I want to share that letter. It was addressed to *"Open letter to EU Member States on the proposed CSA regulation"* and read:

> *Dear Ministers and Ambassadors of EU Member States, We, the undersigned European enterprises, as well as the European DIGITAL SME Alliance - which represents more than 45,000 digital Small and Medium Enterprises across Europe, write to you with deep concern regarding the proposed Regulation on Child Sexual Abuse (CSA). Protecting children and ensuring that everyone is safe on our services and on the internet in general is at the core of our mission as privacy-focused companies. We see privacy as a fundamental right, one that underpins trust, security and freedom online for adults and children alike. However, we are convinced that the current approach followed by the Danish Presidency would not only make the internet less safe for everyone, but also undermine one of the EU's most important strategic goals: progressing towards higher levels of digital sovereignty.*

Digital sovereignty is Europe's strategic future: *In an increasingly unstable world, Europe needs to be able to develop and control its own secure digital infrastructure, services, and technologies in line with European values. The only way to mitigate these risks is to empower innovative European technology providers. Digital sovereignty matters for two key reasons:*

- ***Economic independence:*** *Europe's digital future depends on the competitiveness of its own businesses. But forcing European services to undermine their security standards by scanning all messages, even encrypted ones, using client-side scanning would undermine users' safety online, and go against Europe's high data protection standards. Therefore European users - individuals and businesses alike - and global customers will lose trust in our services and turn to foreign providers. This will make Europe even more dependent on American and Chinese tech giants that currently do not respect our rules, undermining the bloc's ability to compete.*

- ***National security:*** *Encryption is essential for national security. Mandating what would essentially amount to backdoors or other scanning technologies inevitably creates vulnerabilities that can and will be exploited by hostile state actors and criminals. For this exact reason, governments exempted themselves from the proposed CSA scanning obligations. Nevertheless, a lot of sensitive information from businesses, politicians and citizens will be at risk, should the CSA Regulation move forward. It will weaken Europe's ability to protect its critical infrastructure, its companies, and its people.*

The CSA Regulation will undermine trust in European businesses

Trust is Europe's competitive advantage. Thanks to the GDPR and Europe's strong data protection framework, European companies have built services that users worldwide rely on for data protection, security, and integrity. This reputation is hard-earned and gives European-based services a unique selling point which Big Tech monopolies will never be able to match. This is one of the few, if not the only competitive advantage Europe has over the US and China in the tech sector … but the CSA Regulation risks reversing this success.

This legal text would undermine European ethical and privacy-first services by forcing them to weaken the very security guarantees that differentiate European businesses internationally. This is particularly problematic in a context where the US administration explicitly forbids its companies to weaken encryption, even if mandated to do so by EU law. Ultimately, the CSA Regulation will be a blessing for US and Chinese companies, as it will make Europe kill its only competitive advantage and open even wider the doors to Big Tech.

The EU has committed itself to strengthening cybersecurity through measures such as NIS2, the Cyber Resilience Act, and the Cybersecurity Act. These policies recognize encryption as essential to Europe's digital independence. The CSA Regulation, however, must not undermine these achievements by effectively mandating systemic vulnerabilities.

It is incoherent for Europe to invest in cybersecurity with one hand, while legislating against it with the other.

European Small and medium-sized enterprises (SMEs) would be hit hardest if obliged to implement client-side scanning. Unlike large technology corporations, SMEs often do not have the financial and technical resources to develop and maintain intrusive surveillance mechanisms, meaning compliance would impose prohibitive costs or force market exit. Moreover, many SMEs build their unique market position on offering the highest levels of data

protection and privacy; which particularly in Europe is a decisive factor for many to choose their products over the counterparts of Big Tech. Mandating client-side scanning would undermine this core value proposition of many European companies.

This will suffocate European innovation and cement the dominance of foreign providers. Instead of building a vibrant, independent digital ecosystem, Europe risks legislating its own companies out of the market.

For these reasons, we call on you to:

- *Reject measures that would force the implementation of client-side scanning, backdoors, or mass surveillance of private communications, such as we currently see in the Danish proposal for a Council position on the CSA Regulation.*
- *Protect encryption to strengthen European cybersecurity and digital sovereignty.*
- *Preserve the trust that European businesses have built internationally.*
- *Ensure that EU regulation strengthens, rather than undermines, the competitiveness of European SMEs.*
- *Pursue child protection measures that are effective, proportionate, and compatible with Europe's strategic goal of digital sovereignty.*

Digital sovereignty cannot be achieved if Europe undermines the security and integrity of its own businesses by mandating client-side scanning or other similar tools or methodologies designed to scan encrypted environments, which technologists have once again confirmed cannot be done without weakening or undermining encryption. To lead in the global digital economy, the EU must protect privacy, trust, and encryption.

And this letter was then signed by 40 of Europe's larger tech companies. One line stood out for me in that letter: *"This is particularly problematic in a context where the US administration explicitly forbids its companies to weaken encryption, even if mandated to do so by EU law."*

That feels like a response to the UK's order to Apple which was loudly and publicly rebuffed when Tulsi Gabbard, the U.S. Director of National Intelligence tweeted on 'X' that as a result of the U.S. administration's closely working with the UK, Americans' private data would remain private and our Constitutional rights and civil liberties would be protected. She stated in that tweet that *"As a result, the UK has agreed to drop its mandate for Apple to provide a 'back door' that would have enabled access to the protected encrypted data of American citizens and encroached on our civil liberties."* Unfortunately, it's believed that the UK has since issued another "order" to Apple, requiring that it allow the government access to the iCloud data of its own citizens. We'll how that one plays out.

Overall, though, I think that the Open Letter made a very good point about the fundamental competitive disadvantage that the entire EU sector would face if its companies were forced to abide by a privacy invading law – which the members of its own government had conveniently excluded themselves from – while the rest of the world was not laboring under the same regulations.

The UK still needs to be backed away from the spying-on-its-own-citizens precipice, but there are encouraging signs that this might all workout in the end.

Salesforce says it won't pay extortion demand in 1 billion records breach
Last week we showed the ransom demand posting to BreachForum by the Scattered LAPSUS$ Hunters group. Salesforce's public response was widely covered in the tech press. Here's what Dan Goodin wrote for Ars Technica:

Salesforce says it's refusing to pay an extortion demand made by a crime syndicate that claims to have stolen roughly 1 billion records from dozens of Salesforce customers.

Google's Mandiant group said in June that the threat group making the demands began their campaign in May, when they made voice calls to organizations storing data on the Salesforce platform. The English-speaking callers would provide a pretense that necessitated the target connect an attacker-controlled app to their Salesforce portal. Amazingly—but not surprisingly—many of the people who received the calls complied.

The threat group behind the campaign is calling itself Scattered LAPSUS$ Hunters, a mashup of three prolific data-extortion actors: Scattered Spider, LAPSuS$, and ShinyHunters. Mandiant, meanwhile, tracks the group as UNC6040, because the researchers so far have been unable to positively identify the connections.

Earlier this month, the group created a website that named Toyota, FedEx, and 37 other Salesforce customers whose data was stolen in the campaign. In all, the number of records recovered, Scattered LAPSUS$ Hunters claimed, was "989.45m/~1B+." The site called on Salesforce to begin negotiations for a ransom amount "or all your customers' data will be leaked." The site went on to say: "Nobody else will have to pay us, if you pay, Salesforce, Inc." The site said the deadline for payment was last Friday.

In an email Wednesday, a Salesforce representative said the company is spurning the demand.

The representative wrote: "I can confirm Salesforce will not engage, negotiate with, or pay any extortion demand. The confirmation came a day after Bloomberg reported that Salesforce told customers in an email that it won't pay the ransom. The email went on to say that Salesforce had received "credible threat intelligence" indicating a group known as ShinyHunters planned to publish data stolen in the series of attacks on customers' Salesforce portals.

The refusal comes amid a continuing explosion in the number of ransomware attacks on organizations around the world. The reason these breaches keep occurring is the hefty sums the attackers receive in return for decrypting encrypted data and/or promising not to publish stolen data online. Security firm Deepstrike estimated that global ransom payments totaled $813 million last year, down from $1.1 billion in 2023.

The group that breached drug distributor Cencora alone received a whopping $75 million in ransomware payments, Bloomberg reported, citing unnamed people familiar with the matter.

Making ransomware payments has come increasingly under fire by security experts who say the payments reward the bad actors responsible and only encourage them to pursue more riches. Independent researcher Kevin Beaumont wrote on Mastodon, referring to the UK's National Crime Agency: "Corporations should not be directly funding organized crime with the support of the National Crime Agency and their insurance. Break the cycle." Beaumont said in an interview that while the NCA publicly recommends against paying ransoms, multiple organizations he's talked to report having NCA members present during ransom negotiations.

On Mastodon, Kevin warned that payments pose threats to broader security, writing: "It's becoming a real mess to defend against this stuff in the trenches, let me tell you. I am concerned about where this is going."

I imagine Kevin is worried because there's no end in sight. The bad guys have figured out that the human factor is reliably the weakest link in the enterprise security chain. This gets the attackers inside the enterprise, and enterprise networks are not currently hardened against abuse from the inside.

Among the approximately 39 companies believed to have been breached due to their customer relationship with Salesforce, Salesloft and Drift, is the Australian airline Qantas – that we talked about last week with its looney injunction against anyone republishing their data after it leaks – and also reportedly the Australian Telco Telstra, although Telstra is denying the CyberDaily report.

Unfortunately, these ransomware groups are compelled to release the data they have obtained once they've made such a public spectacle of their data breach. They cannot ever be seen to be bluffing or making empty threats or they'll lose their ability to threaten. So I imagine that next week we'll be seeing stories of nearly one billion records of data from around 39 major Salesforce customers being leaked online. The bad guys need to leak the data so that their next victim will take them seriously.

Hackers claim Discord breach exposed data of 5.5 million users

Since my initial reporting of the Discord breach last week additional troubling details have surfaced. BleepingComputer reports this significant breach at Discord, though the attacker's and Discord's numbers don't agree. BleepingComputer reported:

Discord says they will not be paying threat actors who claim to have stolen the data of 5.5 million unique users from the company's Zendesk support system instance. The stolen data includes government IDs and partial payment information for some people.

The company is also pushing back on claims that 2.1 million photos of government IDs were disclosed in the breach, stating that approximately 70,000 users had their government ID photos exposed.

Oh, well then. That's so much better. Only 70,000 users had the photos of their government IDs fall into the hands of criminals. BleepingComputer continues:

While the attackers claim the breach occurred through Discord's Zendesk support instance, the company has not confirmed this and only described it as involving a third-party service used for customer support. Discord told BleepingComputer in a statement: "First, as stated in our blog post, this was not a breach of Discord, but rather a third-party service we use to support our customer service efforts. Second, the numbers being shared are incorrect and part of an attempt to extort a payment from Discord. Of the accounts impacted globally, we have identified approximately 70,000 users that may have had government-ID photos exposed, which our vendor used to review age-related appeals. Third, we will not reward those responsible for their illegal actions."

In a conversation with the hackers, BleepingComputer was told that Discord is not being transparent about the severity of the breach, stating that they stole 1.6 TB of data from the company's Zendesk instance.

According to the threat actor, they gained access to Discord's Zendesk instance for 58 hours beginning on September 20, 2025. However, the attackers say the breach did not stem from a vulnerability or breach of Zendesk but rather from a compromised account belonging to a support agent employed through an outsourced Business Process Outsourcing (BPO) provider used by Discord. As many companies have outsourced their support and IT help desks to BPOs, they have become a popular target for attackers to gain access to downstream customer environments.

The hackers allege that Discord's internal Zendesk instance gave them access to a support application, known as Zenbar, that allowed them to perform various support-related tasks, such as disabling multi-factor authentication and looking up users' phone numbers and email addresses. Using access to Discord's support platform, the attackers claimed to have stolen 1.6 terabytes of data, including around 1.5 TB of ticket attachments and over 100 GB of ticket transcripts.

The hackers say this consisted of roughly 8.4 million tickets affecting 5.5 million unique users, and that about 580,000 users contained some sort of payment information. The threat actors themselves acknowledged to BleepingComputer that they are unsure how many government IDs were stolen, but they believe it is more than 70,000, as they say there were approximately 521,000 age-verification tickets.

The threat actors also shared a sample of the stolen user data, which can include a wide variety of information, including email addresses, Discord usernames and IDs, phone numbers, partial payment information, date of birth, multi-factor authentication related information, suspicious activity levels, and other internal information.

The payment information for some users was allegedly retrievable through Zendesk integrations with Discord's internal systems. These integrations reportedly allowed the attackers to perform millions of API queries to Discord's internal database via the Zendesk platform and retrieve further information.

BleepingComputer could not independently verify the hackers' claims or the authenticity of the provided data samples. The hacker said the group demanded $5 million in ransom, later reducing it to $3.5 million, and engaged in private negotiations with Discord between September 25 and October 2.

After Discord ceased communications and released a public statement about the incident, the attackers said they were "extremely angry" and plan to leak the data publicly if an extortion demand is not paid. BleepingComputer contacted Discord with additional questions about these claims, including why they retained government IDs after completing age verification, but did not receive answers beyond the above statement.

No one is going to shed a tear for angry extortionists whose $3.5 million payday fell through. Unfortunately, as I noted in the case of Salesforce, the attackers must now follow through with their threats. I would not want to have my own photo ID out on the Internet circulating among criminals.

Github's high priority migration to Azure's infrastructure.
I suppose it was only a matter of time before Microsoft decided to move its Github property over to their own Azure cloud infrastructure. But the details behind the move will likely be of interest to many of our listeners. The publication *"The Next Stack"* provided the background for this move, writing:

After acquiring GitHub in 2018, Microsoft mostly let the developer platform run autonomously. But in recent months, that's changed. With GitHub CEO Thomas Dohmke leaving the company this August, and GitHub being folded more deeply into Microsoft's organizational structure, GitHub lost that independence. Now, according to internal GitHub documents The New Stack has seen, the next step of this deeper integration into the Microsoft structure is moving all of GitHub's infrastructure to Azure, even at the cost of delaying work on new features.

In a message to GitHub's staff, CTO Vladimir Fedorov notes that GitHub is constrained on capacity in its Virginia data center. He writes: "It's existential for us to keep up with the demands of AI and Copilot, which are changing how people use GitHub." The plan, he writes, is for GitHub to completely move out of its own data centers in 24 months. "This means we have 18 months to execute (with a 6 month buffer)," Fedorov's memo says. He acknowledges that since any migration of this scope will have to run in parallel on both the new and old infrastructure for at least six months, the team realistically needs to get this work done in the next 12 months.

To do so, he is asking GitHub's teams to focus on moving to Azure over virtually everything else. Fedorov wrote: "We will be asking teams to delay feature work to focus on moving GitHub. We have a small opportunity window where we can delay feature work to focus, and we need to make that window as short as possible."

While GitHub had previously started work on migrating parts of its service to Azure, our understanding is that these migrations have been halting and sometimes failed. There are some projects, like its data residency initiative (internally referred to as Project Proxima) that will allow GitHub's enterprise users to store all of their code in Europe, that already solely use Azure's local cloud regions.

"We have to do this," Fedorov writes. "It's existential for GitHub to have the ability to scale to meet the demands of AI and Copilot, and Azure is our path forward. We have been incrementally using more Azure capacity in places like Actions, search, edge sites and Proxima, but the time has come to go all-in on this move and finish it."

GitHub has recently seen more outages, in part because its central data center in Virginia is resource-constrained and running into scaling issues. AI agents are part of the problem. But it's our understanding that some GitHub employees are concerned about this migration because GitHub's MySQL clusters, which form the backbone of the service and run on bare metal servers, won't easily make the move to Azure and lead to even more outages going forward. In a statement, a GitHub spokesperson confirmed our reporting and told us that "GitHub is migrating to Azure over the next 24 months because we believe it's the right move for our community and our teams. We need to scale faster to meet the explosive growth in developer activity and AI-powered workflows, and our current infrastructure is hitting its limits. We're prioritizing this work now because it unlocks everything else. For us, availability is job #1, and this migration ensures GitHub remains the fast, reliable platform developers depend on while positioning us to build more, ship more, and scale without limits. This is about ensuring GitHub can grow with its community, at the speed and scale the future demands."

For some open source developers, having GitHub linked even closer to Microsoft and Azure may also be a problem; though for the most part, some of the recent outages and rate limits developers have been facing have been the bigger issue for the service. Microsoft has long been a good steward of GitHub's fortunes, but in the end, no good service can escape the internal politics of a giant machine like Microsoft, where executives will always want to increase the size of their fiefdoms.

To me, this makes sense for Microsoft but it also sounds as though it's going to be more easily said than done. And the thing about unforeseen consequences, is that they're unforeseen. And outages for any service such as Github, upon which so much depends, are going to be a problem. But no one sees another way. I have the feeling that future Security Now podcasts will be reporting on the consequences of this move.

California enacts law giving consumers ability to universally opt out of data sharing

I've been noting that the proper place for consumers to specify how they would like the Internet to treat them is in their browser. That was what I loved so much about the original DNT "Do Not Track" beacon. With a flip of a switch just once, a user could configure their web browser to always append a DNT header to every Internet resource request and – had anyone ever cared to honor that request – that would have been their "one and done" prohibition against tracking.

Because this broad concept has merit, the newer incarnation of DNT is GPC – the Global Privacy Control – (https://globalprivacycontrol.org/). But even though the GPC signal has been around for a while, only Brave, the DuckDuckGo and Tor browsers are broadcasting it be default. Firefox since release 95 has supported GPC but it needs to be turned on. Sadly, and perhaps not surprisingly, there is no support for GPC from the various other Chromium-based browsers: Chrome, Edge, Vivaldi and Opera. Anyone wishing to emit the GPC signal from any Chromium-based browser other than Brave will need to install an add-on. And there's also been no sign of GPC from Safari.

So all of that makes the news of California's new legislation last Wednesday all the more important and significant. The Record reported:

*California Governor Gavin Newsom on Wednesday signed a bill which **requires*** [that's right, requireds] *web browsers to make it easier for Californians to opt-out of allowing third parties to sell their data.*

The California Consumer Privacy Act, signed in 2018, gave Californians the right to send opt-out signals, but major browsers have not had to make opt-outs simple to use. The bill signed Wednesday requires browsers to set up an easy-to-find mechanism that lets Californians opt-out with the push of a button, instead of having to do so repeatedly when visiting individual websites.

Privacy and consumer rights activists have been nervously waiting for Newsom to sign the bill, which passed the California legislature on September 11. This is the first law in the country of its kind. The governor vetoed a similar but broader bill last year which also applied to mobile operating systems. Matt Schwartz, a policy analyst at Consumer Reports said: "These signals are going to be available to millions more people and it's going to be much easier for them to opt out."

Until now, Schwartz said, individuals who want to use a universal opt out have had to download third party browser extensions or use a privacy protective browser. [Meaning Brave, DuckDuckGo, Tor or Firefox]

Other bills signed by Newsom on Wednesday also give Californians important data privacy rights. One of them requires social media companies to make it easy to cancel accounts and mandates that cancellation lead to full deletion of consumers' data. A second bolsters the state's Data Broker Registration Law by giving consumers more information about what personal data is collected by data brokers and who can obtain it.

I did some additional research and found that this was measure "AB 566" relating to "Opt-Out Preference Signals". Unfortunately, it appears that we're not going to be getting it for another 14 months since the new law doesn't take effect until January 1, 2027. But at that time, all web browsers will need to include functionality for Californians to send an opt-out preference signal to businesses they visit online through the browser. The law follows the California Privacy Protection Agency (CPPA) announcement of a joint investigative sweep with privacy enforcers in Colorado and Connecticut to investigate potential noncompliance with the Global Privacy Control.

So, at least we have some progress. Chromium browsers will need to get with the GPC plan, as will Safari. And once we have GPC available, privacy enforcers will be able to start investigating who is and who is not honoring the clear preference setting that will be sent by all browsers. As we saw with Do Not Track, just having a GPC signal means nothing if there's no penalty for ignoring it. And while we're at it, how about we also allow our browsers to send a "Cookie Acceptance Preference" signal so that we can dispense with all of those ridiculous cookie permission pop-ups?

OpenAI says they're blocking Chinese misuse

Last Tuesday, OpenAI posted a piece titled "Disrupting malicious uses of AI". This pointed to a detailed and lengthy 37-page report about their efforts to block many different abuses of their technology. Among those cited, OpenAI moved to disrupt PRC espionage operations. Their security team banned ChatGPT accounts used by Chinese state-sponsored hackers to write spear-phishing emails. The accounts were allegedly used by groups tracked by the infosec industry as UNK_DROPPITCH and UTA0388. The emails targeted Taiwan's semiconductor industry, US academia, US think tanks, and organizations representing Chinese minorities. OpenAI says threat actors primarily abuse its service to improve phishing messages, rather than write malware, which is also what threat intel company Intel471 has observed.

This is certainly a good thing. But I suppose I'm not hugely impressed because OpenAI was likely being used only because it was among the lowest hanging fruit. There are so many other sources of the same or similar generative AI assistance that this feels like a battle that will always be lost. Many others won't care, especially if they can generate some income from that abuse of their services.

Microsoft makes IE Mode even harder to access

It would be difficult to find a better example of the need to continue supporting long past its prime website code, than is evidenced by the fact that Microsoft continues to need to offer the option to reload very old web pages under creaky old "IE Mode". It's true. What's also true is that IE's old the "Chakra" JavaScript interpreter contains exploitable flaws that bad guys want access to.

We're talking about this ancient history today because it's apparently less ancient than we might hope. IE Mode is still being exploited to the point that Microsoft's most recent iteration of Edge has removed all easy-to-click buttons from the browser's UI.

An unknown threat actor has been tricking Microsoft Edge users into enabling Internet Explorer mode in Edge to run malicious code in a user's browser and take over their device. These mysterious attacks have been conducted since at least August, according to the Microsoft Edge security team.

IE legacy mode, or IE Mode, is a separate website execution environment within Edge. It works by reloading a web page, but running the reloaded page and its code inside the old Internet Explorer engines. As we know, Microsoft included IE mode in Edge when it retired its predecessor. This allowed Edge to indirectly run old websites and government portals coded decades ago. To access a site under IE Mode users must press a button or menu option to reload the page from Edge into the old IE execution environment.

Microsoft has said that it received "credible" reports that hackers were using clones of legitimate websites to instruct users to reload the clones in the Edge IE Mode. When that happened the malicious site would execute an exploit chain targeting IE's creaky old Chakra JavaScript engine. The exploit chain contained a Chakra zero-day that allowed them to run malicious code, and a second exploit to elevate privileges and take over the entire user platform.

In response, Microsoft did not assign a CVE nor release a patch. Instead, they overhauled the entire IE Mode. The Edge security team has completely removed all the dedicated buttons that could once easily refresh and relaunch a website in IE Mode. This includes the dedicated toolbar button, the context menu option, and the hamburger (main) menu item.

From this point on, anyone wishing to relaunch a website in IE Mode will have to first go into the browser's settings and specifically enable the normally disabled feature there. They'll then be required to relaunch their browser and manually add the URL of a website to an allowlist of sites permitted to be reloaded in IE Mode. It sure sounds as though Microsoft is none too happy that their old Internet Explorer code is still coming back to bite them, so they've decided that while they still cannot safely just kill it off once and for all, at least they can really make it much more difficult to use ... and thus abuse.

Salesforce customer data starting to leak

Remember how I was saying that we were almost certainly going to soon be hearing news of the leaks of Salesforce customer data? Just during the time I was assembling today's show, the news broke that the first tranche of those nearly 1 billion leaked Salesforce customer records has been published. Top of the list was Quantas Airlines – gee, the criminals were not dissuaded by that permanent injunction the Quantas CEO managed to obtain from Australia's Supreme Court. Joining Quantas in private database publication we also have Vietnam Airlines, Albertson's, The Gap, FujiFilm and Engie Resources.

In the case of Vietnam Airlines, who we're mentioning for the first time, the Scattered Lapsus$ Hunters group leaked 7.3 million details from Vietnam Airlines customer loyalty program, that data having been taken from the company's Salesforce account.

The mess created by Texas' new SB2420 legislation
Last Wednesday, Apple's developer portal posted their position and response to the Texas' Senate's Bill SB2420 whose full official title is: *"Relating to the regulation of platforms for the sale and distribution of software applications for mobile devices."*

There's been a lot of recent child protective legislation activity in Texas recently, so things can get a bit confusing. So first, to clarify, this Senate Bill 2420 legislation, which Apple is responding to, is not the same bill that recently caused Pornhub to go dark across Texas. Pornhub suspended its services in Texas because of a Texas law passed two years ago, in 2023, House Bill HB 1181. It was immediately challenged in the courts and wound up surviving. That's the law that requires websites hosting a majority of content that's inappropriate for minors to proactively verify the age of every single visitor before they are allowed in. Lacking any accepted privacy-enforcing means to do that, and given that we're now seeing tens of thousands of extremely personal government ID scans falling into criminal hands during data breaches (which appear to be inevitable), Pornhub probably correctly determined that the percentage of people who would be willing to be fully deanonymized during their visits to their site would not be appreciable. So just closing their doors to Texans was the right solution.

It's worth mentioning that this Texas legislation HB1181, now having survived the courts, all the way up to the U.S. Supreme Court, is likely to become a model for other states' legislation which will therefore not need to struggle for adoption and enforcement. So we might expect to see many other states driving adult content websites out of their jurisdictions simply by following Texas' lead. But back to Texas newer legislation, which is Senate Bill SB2420...

While its official title is *"Relating to the regulation of platforms for the sale and distribution of software applications for mobile devices"*, it is commonly referred to as the *"App Store Accountability Act."* It regulates how app stores and software application developers operating in Texas must verify user ages and handle purchases or downloads by any minors in the state.

The legislation states that the owners and operators of App stores must verify a user's age via a *"commercially reasonable method"* when an account is created. If a user is a minor (under 18, as defined in the bill), the legislation requires that the minor's account be tied to ("affiliated" with) a parent's or guardian's account. Additionally, each download or purchase by a minor must first receive explicit parental consent.

The store must also clearly and conspicuously display each app's age rating and the content elements that were used to derive that rating. App stores must limit their data collection to what is needed for obtaining age verification, consent, and recordkeeping. And any violations of any of these provisions such as attempts to obtain blanket consent or making any misrepresentations can be treated as deceptive trade practices.

So that's on the app store side. Software developers have obligations under this new legislation as well. Developers must assign an age rating to each of their apps, including any in-app purchases. And those age assignments must be consistent with the age categories specified in the bill. Developers much also substantiate their age assignments by providing the app content elements which lead to that rating. They must notify app stores of any significant changes to the app's terms, its privacy policy, changes in monetization or features, or any change in the app's resulting rating.

Apps must use the age and consent information from the app store to enforce age restrictions, to comply with the law and enable any safety features. Apps must delete any personal data received for age verification once such verification is completed. And any violations such as misrepresenting the app's age rating, enforcing terms against minors without consent, wrongful

disclosure of personal data, and such are actionable. However, there are some liability protections. If the developer follows widely adopted industry standards in good faith, this new Texas law states that they may be exempt from liability.

Until we had this new Texas law, which was signed into law by Texas Governor Greg Abbott and is scheduled to take effect on January 1, 2026, so in less than three months, app store and application age and content ratings were advisory only. App stores run by Apple and Google were assigning age ratings to apps using self-regulatory frameworks such as the IARC (International Age Rating Coalition) system. Developers answered questionnaires about their apps, the stores would generate an age rating such as "12+" or "Teen", and display those indications. But all of those were informational only. Nothing prevented app acquisition and download by younger users. That's the big thing that SB2420 has changed.

Now, app developers are legally required to assign an age rating using criteria defined by this Texas law. App stores must display those ratings and the specific content descriptors. And these ratings now carry legal weight and must be enforced by app store technology to trigger parental-consent requirements and enable or disable the app's download. And any developer who mis-rates an app or fails to update ratings after material changes can face liability under deceptive trade-practice law.

Naturally, Apple, who sees privacy concerns hiding around every corner, has not been happy about any of this. In fact, Tim Cook is believed to have called Greg Abbott to argue against the provisions of the legislation, asking Abbott to either modify or completely veto the Bill. Those pleas apparently fell on deaf ears. Apple's concerns have been that the new law would require "sensitive, personally identifying information" to be collected from any Texan who wants to download apps, even innocuous ones such as weather apps, sports scores, etc. And Apple has warned of downstream data sharing since SB 2420 requires app stores to implicitly share age and parental consent status with developers.

And, of course, the bottom line is that Apple really really really **really** doesn't want to do this or get involved in any way with any of this. However, that does not feel like a practical long-term position for Apple to be taking. Everything we see everywhere, evidences a growing awareness of age-related Internet content control.

Okay. So I started out by noting that last Wednesday, Apple's developer portal posted their position and response to these new Texas requirements. Apple's posting was titled *"New requirements for apps available in Texas"*, and Apple writes:

> *Beginning January 1, 2026, a new state law in Texas — SB2420 — introduces age assurance requirements for app marketplaces and developers. While we share the goal of strengthening kids' online safety, we are concerned that SB2420 impacts the privacy of users by requiring the collection of sensitive, personally identifiable information to download any app, even if a user simply wants to check the weather or sports scores. Apple will continue to provide parents and developers with industry-leading tools that help enhance child safety while safeguarding privacy within the constraints of the law.*
>
> *Once this law goes into effect, users located in Texas who create a new Apple Account will be required to confirm whether they are 18 years or older. All new Apple Accounts for users under the age of 18 will be required to join a Family Sharing group, and parents or guardians will need to provide consent for all App Store downloads, app purchases, and transactions using Apple's In-App Purchase system by the minor. This will also impact developers, who will need to adopt new capabilities and modify behavior within their apps to meet their obligations under*

the law. Similar requirements will come into effect later next year in Utah and Louisiana.

Yeah... and just wait until Mississippi gets wind of this and figures out that they can do the same thing! Apple continued:

Today, we're sharing details about updates we're making and the tools we'll provide to help developers meet these new requirements.

To assist developers in meeting their obligations in a privacy-preserving way, we'll introduce capabilities to help them obtain users' age categories and manage significant changes as required by Texas state law. The ***Declared Age Range API*** *is available to implement now, and will be updated in the coming months to provide the required age categories for new account users in Texas. And new APIs launching later this year will enable developers, when they determine a significant change is made to their app, to invoke a system experience to allow the user to request that parental consent be re-obtained. Additionally, parents will be able to revoke consent for a minor continuing to use an app. More details, including additional technical documentation, will be released later this fall.*

We know protecting kids from online threats requires constant vigilance and effort. That's why we will continue to create industry-leading features to help developers provide age-appropriate experiences and safeguard privacy in their apps and games, and empower parents with a comprehensive set of tools to help keep their kids safe online.

https://developer.apple.com/documentation/declaredagerange/

So I went over to check out Apple's *"Declared Age Range"* API. The page is titled *"Declared Age Range: Create age-appropriate experiences in your app by asking people to share their age range."* I was struck by the language *"by asking people to share"* and by the name of the entire API, which is, after all, the "Declared Age Range" API. What follows, then, is the "Overview" of the API, which says:

Use the Declared Age Range framework to request people to share their age range with your app. For children in a Family Sharing group, a parent or guardian, or the Family Organizer can decide whether to always share a child's age information with your app, ask the child every time, or never share their age information. Along with an age range, the system returns an AgeRangeService.AgeRangeDeclaration for the age range a person provides.

And then, in a vividly highlighted callout box labeled "Important", the page states:

Data from the Declared Age Range API is based on information declared by an end user, or their parent or guardian. You are solely responsible for ensuring compliance with associated laws or regulations that may apply to your app.

"You (the developer to whom this page is addressed) are solely responsible for ensuring compliance with associated laws or regulations that may apply to your app."

Yikes. So this is Apple saying that all they are doing is functioning as a middleman, to pass along whatever age declaration the user might assert and that the app's developer remains responsible for ensuring compliance with associated laws or regulations. This, of course, begs the question,

what does the forthcoming Texas SB2420 law require in that regard? We know that in other jurisdictions and contexts self-declaration of age is specifically regarded as insufficient. So what about in Texas? The bill does not mandate a single specific age-verification method, such as uploading an ID, but it does require app stores to use a *"commercially reasonable method"* to verify a user's age — not just accept whatever age the user may self- declare.

As clarifying examples, the legislation states that app stores may not rely on a birth date entered into a form or any other method that is *"reasonably likely to be circumvented by a minor."*

I've been studying this carefully in an attempt to understand how and whether Apple's "Declared Age Range" API is in any way sufficiently responsive to what Texas requires. It certainly does not appear to be. The only way I can see that it could be applicable be would be if Apple starts out with "Declared Age" then later replaces the "declaration" part with a full responsibility-taking verifiable age determination mechanism. In that way, the same API could be used and just the source of the age determination information would change. So, for example, that would be done state-by-state or political jurisdiction by jurisdiction. This would allow self-declaration to continue to be sufficient within regions that have not yet clamped down on their citizens, and only using (and requiring) verifiable age verification where the governing laws require its use.

What Apple has today with their Apple Family Sharing is that Apple asks for a date of birth during account creation. For accounts under 13, Apple requires an adult parent to be a member of the Family Group. And for ages 13–17, a teen can create their own Apple ID without parental verification with Apple trusting the date entered. That all dies in Texas on New Years Day.

What's required by Texas SB2420, is an affirmative "commercially reasonable method" of age verification for **every** account. Self-declaration is never sufficient. This implies that for Texas users, Apple will need to implement some new form of age verification; ID checks, credit-card based validation, or some other form of verifiable age-assurance technology. And Apple has fewer than three months to bring that online. While Apple currently only requires and enforces parental linking for account owners younger than 13, SB2420 applies to **all minors under 18.**

Under Apple's current Family Sharing plan, the "Ask to Buy," option is available to parents who may choose to enable it, but it can be disabled, and parents can also choose to grant blanket permissions. Under SB2420, blanket or any form of pre-authorized permission is expressly forbidden. Under SB2420, parental consent is legally required for **every** app download and in-app purchase by any minor. Imagine being a 17 year old High School senior in Texas, and needing to obtain your mother's permission to add an app – any app, regardless of its age rating – to your iPhone. What a mess.

The language of the law states: *"…an operator of a digital distribution platform [app store] shall obtain verifiable parental consent before allowing a minor to download or purchase any software application through the platform."* and also *"Parental consent must be obtained on a per-transaction basis, and may not be granted as a blanket authorization."* It's not difficult to see why Tim Cook would have given Greg Abbott a call to plead with him to amend or to veto this legislation.

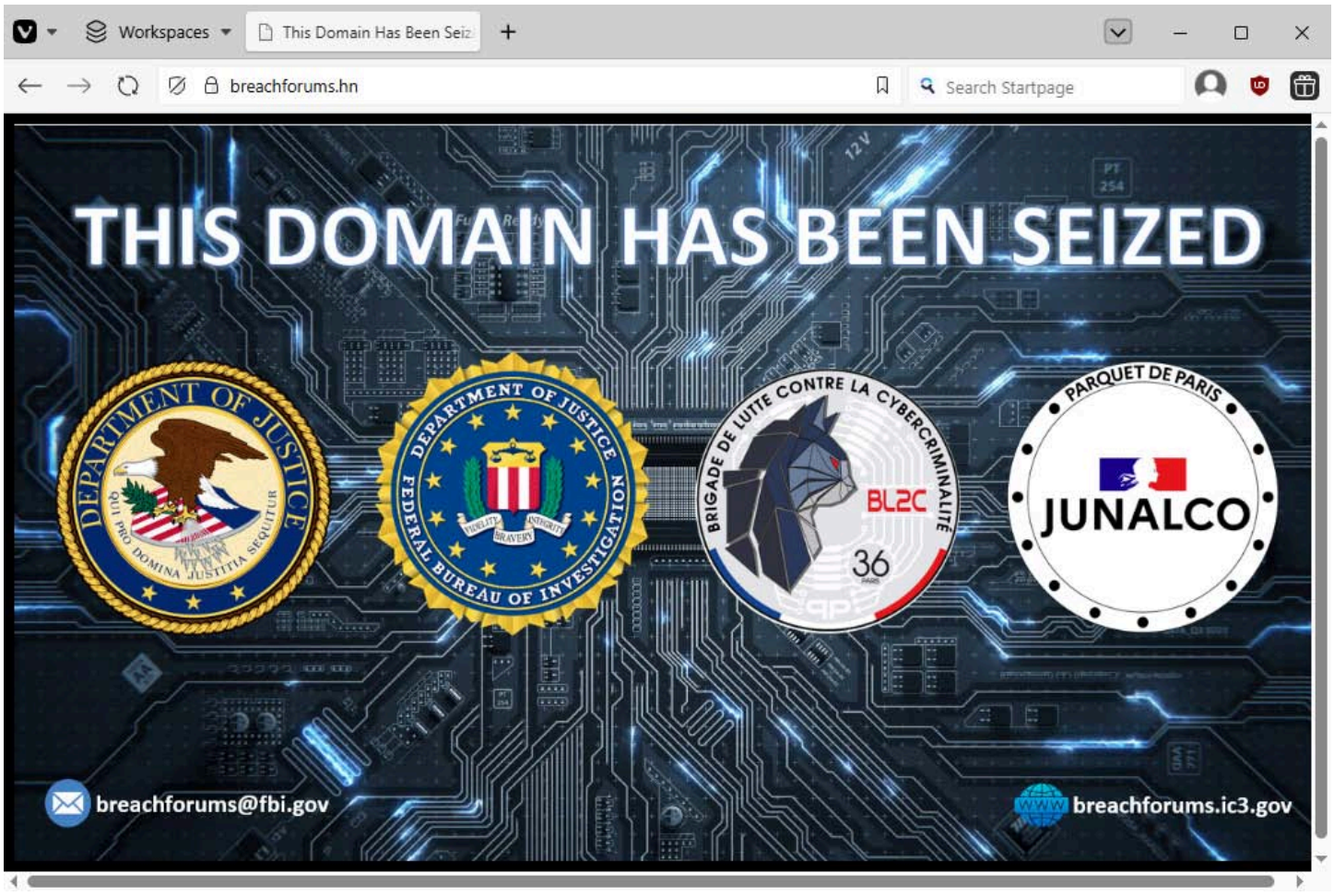
One interesting aspect of the legislation is that nothing in it appears to apply retroactively. The age verifications are only performed upon new account creation. However, existing adult accounts might need to have their adult status reasserted if a minor's account were to be linked to it as a parent or guardian.

Whatever the case, this new Texas SB2420 legislation is going to create a mess, and it's only about 10 weeks away from coming into effect. So far, the law has not been challenged in court, perhaps because Texas' earlier HB1181 legislation survived both the 5th Circuit Court of Appeals and then the U.S. Supreme Court. So under the current U.S. legal climate it might be viewed as a fait accompli that's not worth fighting.

This leaves us with the question: How is Apple going to verifiably determine the ages of any new account holders in Texas? Perhaps an age verification will simply be performed at the time of any new iPhone purchase.

BreachForums gets a makeover

Last week's show notes showed the Scatters LAPSUS$ Hunters' "BreachForums.hn" website from which I read the extortion demand directed at Salesforce. That demand explained that if only the Salesforce folks would negotiate with them the unfortunate disclosure of the nearly one billion records of their customer's information could be averted. I wanted to note that **this week** that BreachForums.hn website has a brand new look:



"Hn" is the top level domain for the Central American country of Honduras and the FBI has taken over that domain's DNS, pointing it to one of its own landing pages.

Widespread RDP infrastructure attack underway

Greynoise has detected and reported a widespread Botnet-driven attack, which began last

Wednesday October 8th, sourced by more than 100,000 individual bots scattered across the globe, all aimed at U.S. based exposed RDP endpoints.

As we know all too well, RDP is Microsoft's very poorly authenticated Remote Desktop Protocol which keeps being used because it works so well and is so incredibly handy. Unfortunately, it has also been an unending source of remote network intrusions through the years as bugs and other various failings have continually been found in its code. I love RDP. It does work incredibly well and I use the crap out of it. But nowhere among any of GRC's Internet-facing IPs and ports will anyone ever find any exposed RDP service because for me – or anyone – to publicly expose any instance of RDP to the Internet would just be begging for an intrusion. I have three words: Don't do it.

Unfortunately, my repeated admonishment flies in the face of convenience. And as we know, convenience often trumps security. *"But why would the great and powerful Microsoft allow us to turn it on if it wasn't secure? And my god it's so handy!"* Right. A Shodan search for "Remote Desktop Protocol" returns on the order of 2.4 Million results. Some sources have claimed that Shodan has indexed more than 3.5 million exposed RDP ports, and some non-Shodan research has shown 4,493,357 exposed RDP services when scanning for RDP running on it's default port of 3389.

All of this; all of this RDP nonsense, is very nicely covered by one of the most important lessons all of us who have been participating together in this podcast for the past 20 years have learned: Authentication is generally broken and should never be trusted. The only Internet servers that should ever be placed onto the Internet are those that do not use any authentication. Authentication that's never used can never be broken – because there isn't any. So things like web servers and DNS servers and email servers which are designed to be accessible by anyone – whose entire purpose is that they are for use by anyone, anywhere – they are safe to deploy. But anything that requires any form of authentication is inherently risky.

The only exception to that is that I would be inclined to trust well-tested and carefully vetted connections to SSH servers running on a non-standard port only if those connections are authenticated with cryptographically secure certificate credentials. But even there, wherever possible, filter all incoming connections by region. If you never roam outside of your own country, why would you ever entertain connections from China, Russia or Iran? None of whom are friends of the West? Don't even consider accepting their traffic to your non-public servers. Use some geofencing to drop any traffic coming in to authenticating endpoints if its IP is foreign.

Greynoise wrote:

> *Since October 8, 2025, GreyNoise has tracked a coordinated botnet operation involving over 100,000 unique IP addresses from more than 100 countries targeting Remote Desktop Protocol (RDP) services in the United States. The campaign employs two specific attack vectors — RD Web Access timing attacks and RDP web client login enumeration — with most participating IPs sharing one similar TCP fingerprint, indicating centralized control. Source countries include Brazil, Argentina, Iran, China, Mexico, Russia, South Africa, Ecuador, and more than 92 others.*

I would only ask that everyone consider filtering and dropping any traffic coming into any non-public authenticating services. You know you don't need or want that traffic. You should never assume that your authentication will hold. Blocking and dropping traffic that you know you don't want is what firewalls are for. But firewalls won't help if they are not used.

Listener Feedback

Dan Linder

This well respected UI/UX organization agrees the new iOS 26 interface is a mess. They clearly describe a lot of our feelings well. I hope Apple listens.
https://www.nngroup.com/articles/liquid-glass/ */ Dan*

Dan is, of course, posting this in at least partial response to last week's UI rant where I detailed my feelings about the unproductive nonsense that Apple had added to their user interface, forgetting the #1 rule of UI design, which is that the interface should never call attention to itself for its own sake and should do everything it can to disappear and facilitate the user's use.

The brief TL;DR summary at the top of the wonderful takedown piece reads: *"iOS 26's visual language obscures content instead of letting it take the spotlight. New (but not always better) design patterns replace established conventions."* The piece begins:

With iOS 26, Apple seems to be leaning harder into visual design and decorative UI effects — but at what cost to usability? At first glance, the system looks fluid and modern. But try to use it, and soon those shimmering surfaces and animated controls start to get in the way. Let's strip back the frost and look at how these changes affect real use.

iOS 26 introduces Apple's new glassmorphic visual language into its phones. Apple describes Liquid Glass as: "a translucent material that reflects and refracts its surroundings, while dynamically transforming to help bring greater focus to content, delivering a new level of vitality across controls, navigation, app icons, widgets, and more."

Translated: the interface now ripples and shimmers as if your phone were encased in Jell-O. At first glance, it does look cool. But problems arise as soon as you start actually using your phone.

Transparency = Hard to See: Liquid Glass makes UI elements translucent and bubbly. The result is light, airy — and often invisible. One of the oldest findings in usability is that anything placed on top of something else becomes harder to see. Yet here we are, in 2025, with Apple proudly obscuring text, icons, and controls by making them transparent and placing them on top of busy backgrounds.

Text on top of images is a bad idea because the contrast between the text and the background is often too low. So why does Apple now encourage users to set photos as backgrounds for text messages? The result is that your friend's words are camouflaged against their beach-vacation photo, or worse, their pet's fur. Content may technically be "in focus," but you can't read (or see) it.

And then comes Apple's boldest (or dumbest) experiment: text on top of text. Apparently, designers decided users have eagle vision and infinite patience, because deciphering one line of text written across another is now fair game. Reading an email subject line now requires Dan Brown-level cryptographic decoder skills.

Not only is it illegible — it's also ugly.

And while there's much more more, I'll finish by sharing this piece verbatim from the piece because if you recall my rant last week, you's be inclined to wonder whether I had written this one, too. The section heading is *"Animated Buttons: Motion Without Meaning"* and reads:

> *Animations can be delightful the first time. When used intentionally, they can also be satisfying — creating that feeling when something just "clicks" or "snaps" into place. Our eyes are finely tuned to detect motion, which is why animated buttons grab attention instantly. But delight turns to distraction on the tenth, twentieth, or hundredth time.*
>
> *In iOS 26, controls insist on animating themselves, whether or not the user benefits. Carousel dots quietly morph into the word Search after a few seconds. Camera buttons jerk slightly when tapped. Tab bars bubble and wiggle when switching views, and buttons briefly pulsate before being replaced with something else entirely. It's like the interface is shouting "look at me" when it should quietly step aside and let the real star — the content — take the spotlight.*

Anyway, I thank Dan for sharing another view, posted last Friday, by a group that specializes in UI design. As Dan says, I hope Apple is listening. I'm glad it's possible to turn those superfluous wiggles, jiggles, zips and zings way down to a tolerable level.

RediShell's CVSS 10.0

A trio of researchers at "Wiz" research worked through Trend Micro's Zero Day Initiative to disclose the significant problem they uncovered in REDIS servers which are exposed over the public Internet. We already know from today's episode title that this vulnerability has received the difficult-to-obtain CVSS of 10.0. The reason this has come to the attention of the Internet community is that there are nearly 330,000 publicly-exposed REDIS servers on the Internet with around 60,000 of those requiring no authentication – making them all ripe for exploitation.

REDIS – R.E.D.I.S. Stands for **RE**mote **DI**ctionary **S**erver. It was created in 2009 by Salvatore Sanfilippo, who built it to solve performance issues at his startup. He initially created Redis to improve the performance of a real-time web analytics system. But the speed of an in-memory network accessible dictionary ended up being so useful that it evolved into a standalone open-source project. Since then Redis has evolved beyond a simple key-value cache into a full in-memory data structure server. And it's here to stay.

GRC runs a REDIS server for Windows to improve the performance of its PHP-based webforums. I have my REDIS server bound to the localhost IP 127.0.0.1 and listening on its default port of 6379. So a number of the PHP-based services on that server take advantage of REDIS to improve their performance. What I'm doing differently from 330,000 other instances is that the last thing I would ever think of doing would be binding the REDIS service to any network interface that's connected to the Internet. Historically, there have been thousands of botnet infections and data leaks due to open Redis ports.

So, on the one hand, nothing horrible involving REDIS would be the first time, but what's been found is new. The guys at Wiz research titled their report: *"RediShell: Critical Remote Code Execution Vulnerability (CVE-2025-49844) in Redis, 10 CVSS score"* and their tease was *"Wiz Research discovers vulnerability stemming from 13-year-old bug present in all Redis versions, used in 75% of cloud environments."*

> *Wiz Research has uncovered a critical Remote Code Execution (RCE) vulnerability, CVE-2025-49844 which we've dubbed #RediShell, in the widely used Redis in-memory data structure store. The vulnerability has been assigned a CVSS score of 10.0 - the highest possible severity (note that we have seen this listed as a 9.9 in some places, depending on the source).*
>
> *The vulnerability exploits a Use-After-Free (UAF) memory corruption bug that has existed for approximately 13 years in the Redis source code. This flaw allows a post auth attacker to send a specially crafted malicious Lua script (a feature supported by default in Redis) to escape from the Lua sandbox and achieve arbitrary native code execution on the Redis host. This grants an attacker full access to the host system, enabling them to exfiltrate, wipe, or encrypt sensitive data, hijack resources, and facilitate lateral movement within cloud environments.*
>
> *Given that Redis is used in an estimated 75% of cloud environments, the potential impact is extensive. Organizations are strongly urged to patch instances immediately by prioritizing those that are exposed to the internet.*

On October 3, Redis released a security advisory along with a patched version of Redis. We extend our gratitude to the entire Redis team for their collaboration throughout the disclosure process. We greatly appreciate their transparency, responsiveness, and partnership during this engagement.

In this post, we will provide a high-level overview of our discovery and its implications. Given the prevalence and sensitivity of this vulnerability, we will defer some of the technical details to a future installment, omitting exploit information for now to allow impacted organizations sufficient time to address the vulnerability. Organizations utilizing Redis are strongly encouraged to update their Redis instances to the latest version immediately.

Vulnerability Meets Ubiquity: The Redis Risk Multiplier

The newly disclosed RediShell (CVE-2025-49844) vulnerability in Redis has been assigned a CVSS score of 10.0 - a rating rarely seen, with only around 300 vulnerabilities receiving it in the past year. It's also the first Redis vulnerability to be rated as critical. The score reflects not just the technical severity of remote code execution, but also how Redis is commonly used and deployed. Redis is widely used in cloud environments for caching, session management, and pub/sub messaging. While Redis has had a strong security history, the combination of this flaw and common deployment practices significantly increases its potential impact.

The vulnerability is a Use-After-Free (UAF) memory corruption that allows an attacker to send a malicious Lua script that leads to arbitrary code execution outside Redis's Lua interpreter sandbox, gaining access to the host. The urgency with which you should address this vulnerability depends on how Redis was installed and its exposure level.

Our analysis across cloud environments revealed the extensive scope of this vulnerability:

- *Approximately 330,000 Redis instances are exposed to the internet at the time of this blog post*
- *About 60,000 instances have no authentication configured*
- *57% of cloud environments install Redis as container images, many without proper security hardening*

The official Redis container, by default, does not require authentication. Our analysis shows that 57% of cloud environments install Redis as an image. If not installed carefully, these instances may lack authentication entirely. The combination of no authentication and exposure to the internet is highly dangerous, allowing anyone to query the Redis instance and, specifically, send Lua scripts (which are enabled by default). This enables attackers to exploit the vulnerability and achieve remote code execution within the environment.

Redis instances are also frequently exposed to internal networks where authentication may not be prioritized, allowing any host in the local network to connect to the database server. An attacker with a foothold in the cloud environment could gain access to sensitive data and exploit the vulnerability to run arbitrary code for lateral movement into sensitive networks.

They conclude their report, as they promised, without disclosing any of the critical details behind their discovery because REDIS has been updated to cure this 13 year old vulnerability and because they most want the world to update.

Sadly, we pretty much know how that's going to go. And given that REDIS is a widely used open source project, it will not be difficult for the bad guys to determine what has been broken for the past 13 years and start scouring the Internet for networks to attack and infiltrate. Also, since REDIS is almost ubiquitously available on internal networks, even when instances are not publicly exposed, attackers will be able to scan the internal network for anything answering on port 6379 then see whether they've found a long-ignored instance of REDIS and no one ever bothered to update which would allow them to pivot their attack into that machine to obtain a deeper foothold inside the network.

The Wiz guys – which first demonstrated this during the Berlin Pwn2Own competition, by the way, concluded their write up writing:

> *RediShell (CVE-2025-49844) represents a critical security vulnerability that affects all Redis versions due to its root cause in the underlying Lua interpreter. With hundreds of thousands of exposed instances worldwide, this vulnerability poses a significant threat to organizations across all industries.*
>
> *The combination of widespread deployment, default insecure configurations, and the severity of the vulnerability creates an urgent need for immediate remediation. Organizations must prioritize updating their Redis instances and implementing proper security controls to protect against exploitation.*
>
> *This vulnerability also highlights how deeply today's cloud environments depend on open-source technologies like Redis.*

The biggest heads-up take away for our listeners is to check your own organizations for any creaky older instances of REDIS that might be running. You could simply perform an internal port scan for anything accepting TCP connections over port 6379. If any are found or known, carefully examine and consider who could obtain connections to its services. And, of course, it's always best to keep current with open source releases. In this instance, it could be crucially important.