Number 105 | August 2025

NTT DATA

Radar

The Cybersecurity magazine

Deepfakes, AI, and New Threats That Demand Greater Awareness

By Francisco Javier García Lorente

The technological revolution we are experiencing, driven by artificial intelligence, has opened a new dimension in the cybersecurity landscape. Tools that seemed like science fiction just a few years ago—such as synthetic image generators, cloned voices, or manipulated videos—are now within reach of anyone with an internet connection. While this progress is fascinating, it has also brought with it emerging threats that require more than just technical measures to be countered: they demand genuine awareness from individuals.

One of the most disruptive phenomena is that of deepfakes: AI-generated audiovisual content that impersonates the faces, voices, or expressions of real individuals with alarming precision.

In the field of cybersecurity, this translates into much more sophisticated social engineering attacks, where the appearance of legitimacy is nearly flawless. A simple video seemingly recorded by a CEO requesting an urgent transfer can have a devastating impact if the recipient is not properly trained to detect subtle irregularities.

Added to this is the use of generative language models capable of producing flawless phishing emails, with contextual awareness and personalized using data gathered from social media.We're no longer talking about poorly written emails with obvious mistakes, but about messages that mimic the tone of a previous conversation or the signature of a known individual.

This "professionalization" of attacks requires a qualitative leap in user training—not only to detect obvious threats but to learn to question and verify even what appears trustworthy.

Furthermore, cybercriminals are combining AI with large-scale attack automation. For example, through bots that attempt millions of password combinations (brute force), systems that identify vulnerabilities in real time, or malware that dynamically adapts to the victim's environment to evade detection.

In this context, having an antivirus solution is not enough: awareness, judgment, and secure habits are essential.

This is where training and awareness become a strategic requirement. Organizations must understand that it’s not just about delivering an annual talk on best practices, but about designing continuous cyber journeys—with content tailored to different levels of knowledge, realistic scenarios, and current threats.

Learning must be evolutionary, practical, and emotional: it's essential to connect with the user and make them feel like part of the defense system.

It's vital to teach everyone—from technical profiles to administrative staff—how to recognize warning signs: altered URLs in links, urgent requests for information, subtle changes in language, or even videos where something just doesn’t seem right.

At the same time, policies governing the use of devices, social media, and communication tools must be updated, as the traditional perimeter has vanished with mobility, remote work, and BYOD (Bring Your Own Device).The conclusion is clear: artificial intelligence has raised the level of threats, but it can also be an ally. Algorithms can be used to detect fraud patterns, automate responses, and protect infrastructure.

However, the most important link remains the human one. A conscious, trained, and empowered person is a barrier that is extremely difficult to breach—even for the most advanced AI.

Investing in awareness is not optional; it is a necessity. Because today, more than ever, security begins with each of us.

Francisco J. García Lorente
Cybersecurity Project Manager

Summer in Flames: Cybersecurity Under Pressure

Cyber Chronicle by Diego Turiegano & Juan Jose Rollán

This summer, the heat is not only scorching the streets but also making itself felt in the digital realm. Between June and July 2025, cyberspace has witnessed a wave of cyberattacks that have put key industries, public institutions, and millions of users worldwide on high alert. From halted production plants to massive credential leaks, the summer season once again proves that in cybersecurity, there are no holidays. Below, we review the most notable cyber incidents of recent weeks.

On July 8th, Hero España confirmed a targeted cyberattack that affected its production plant in Murcia, forcing a temporary halt to its industrial operations. Although the company has not disclosed the type of attack, sources close to the matter suggest it may have been a case of ransomware.

The company activated its contingency protocol to minimize the impact and ensure continued supply to its customers. The incident highlights the growing vulnerability of the food industry, even in environments with high technological and regulatory standards.

Also in July, the city council of Melilla suffered a ransomware attack that took 90% of its servers offline, affecting not only administrative and judicial systems but also its backup infrastructure.

The incident, described as “critical” by authorities, is being investigated by the CNI (National Intelligence Center) and the National Cryptologic Center, who suspect the involvement of an advanced actor with specialized knowledge.

On an international scale, an incident in Norway raised serious concern. A group of attackers managed to access the remote control system of a dam at Lake Risevatnet simply by exploiting a weak password.

For four hours, the attackers opened a discharge valve without the operations team noticing. Although no material damage occurred, the incident exposes the fragility of critical infrastructure in the face of basic digital security failures.

In the financial sector, the cybercriminal group Scattered Spider returned to the spotlight this summer by targeting the insurance company Aflac.

Using vishing (fraudulent phone calls) and MFA bombing (abuse of multi-factor authentication), the attackers gained access to internal systems and exfiltrated confidential data from employees and customers.

Although no ransomware was deployed, the reputational damage has been significant and has raised concerns in the insurance sector, one of the hardest hit this year.

But perhaps the most alarming incident due to its scale was the revelation, at the end of June, of a massive file containing more than 16 billion leaked credentials.

This database, compiled from multiple previous breaches, has been shared across underground forums and contains combinations of emails and passwords still active on banking services, social networks, and corporate platforms.

Experts from ESET have warned that the material can be used to automate phishing attacks, identity theft, and unauthorized access. The recommendation: change passwords immediately and enable multi-factor authentication on all sensitive accounts.

In short, the succession of recent incidents reveals that the cybersecurity landscape is facing a period of maximum demand.

The combination of targeted attacks, massive leaks, and breaches in critical infrastructure confirms that the attack surface continues to grow at the same pace as cybercriminals' capabilities.

Far from being a period of reduced activity, summer has proven to be an especially vulnerable time, where operational complacency and lack of foresight can have serious consequences.

Cybersecurity, now more than ever, must be integrated as a transversal and constant axis in the management of any organization.

Diego Turiegano
Cybersecurity Analyst

Juan José Rollán
Cybersecurity Analyst

Call to awareness action

Article by Leire Cubo Arce

Working as a cybersecurity consultant within the Awareness team has given me a unique perspective on cybersecurity. I have had the privilege of working closely with various organizations and their employees, and throughout this experience, I have observed a fundamental truth: effective cybersecurity awareness is not built on fear, but on understanding and empowerment.

Trying to scare people into being secure rarely works in the long run. Instead, when people understand why cybersecurity is relevant to them and feel empowered to act, they become the strongest first line of defense—stronger than any technology can offer. For this, I follow **three main keys**:

- From Personal to Corporate
- Realistic, Non-Punitive Training
- Using Humor and Without Fear

From Personal to Corporate

Often, an employee doesn't want to hear about the **risks facing the company**, no matter how real the threats are or how much they could directly impact their work or even their future. The reality is that, by nature, most people tend to **prioritize personal** matters over corporate ones.

That's why one of the keys to effective awareness is **building from the personal level upward.** Something I've learned is that if we manage to make a person cybersecurity-aware at home, it's very likely they will be the same at work. After all, bad habits don't stay outside the office door. We must start from the premise that employees will always care first about themselves and their closest environment.

To do this, it's crucial **to ground examples in their daily reality**. Humans are naturally somewhat selfish; we pay real attention when a topic affects us directly. When we understand how phishing can affect our own bank accounts or how a virus can damage our personal computer, the message resonates much more deeply.

From that foundation of personal security, it's much easier to connect the dots and show how those same practices and precautions are crucial for the **company's security.**

Realistic and Non-Punitive Training

Another thing I've observed is a significant gap between organizations that care about cybersecurity training and those that don't. The most forward-thinking understand that cybersecurity is not just a technological issue, but also a human one. They recognize that an **uninformed or untrained employee represents a weak link** and a significant risk. Unfortunately, other organizations see awareness as merely a checkbox—something they must fulfill for audits or regulations. This short-sighted view ignores the fact that true security is not achieved solely with tools, but with **informed and vigilant people**.

I see the same dichotomy reflected in employees' perceptions. Often, what they fear most isn't the real threat of a cyberattack, but the **"consequence management" policies** many companies enforce. The fear of retaliation for falling for a phishing simulation, for example, can create anxiety and a defensive attitude, rather than encouraging proactive learning. This punishment mindset distracts from the real danger.

I firmly believe we need to change this mindset. The real fear shouldn't be failing a simulation, but the **possibility that the phishing attempt was real and the devastating consequences** it could have had for both the company and the employee. Using real examples or showing them that what they hear in the news isn't fiction (as they often say, truth is stranger than fiction) and could affect them is how they will truly understand the importance of being informed.

Training of any kind should never be a tool for punishment, but an opportunity for personal and **professional development**. Bad actors will always exist, so each of us must become our own cybersecurity expert.

Using Humor and Without Fear

Thinking about all the awareness talks I've given, there's one factor that always works better than the rest. For awareness to truly take hold, a much more human—and yes, often a bit mischievous—approach is needed; **humor is a powerful tool** to break the ice and keep attention**.** In fact, my training sessions are more successful when, every now and then, I set little "traps": for example, I ask them to scan a QR code that leads to a "malicious" webpage (totally harmless and under my control, of course), then I wink and promise I "won't tell the boss."

These kinds of hands-on, cheeky experiences not only keep their attention but also help them understand that training doesn't have to be boring or delivered by "the typical speaker who drones on." If you manage to connect with your audience and make learning fun, the information will stick in their minds longer. It might even lead them to talk about the experience with coworkers, reaching many more people than initially planned. Adults are just kids in more mature bodies, and like kids, we love sharing things we find interesting with everyone.

Joy, smiling, and having a dynamic, positive attitude will always go further than a robotic, gloomy person who only delivers bad news. Just ask Artificial Intelligence and the many cybersecurity awareness programs that have started to overuse it… How many times have you rolled your eyes when your company assigns you the annual "Security Awareness" course narrated by an artificial avatar? The facts speak for themselves—I even have some of those courses pending myself.

Investment in Cybersecurity Culture: Data That Speaks

Of course, the first step for everything I've shared so far is to put a huge spotlight on investing in cybersecurity awareness programs. According to a 2023 Statista report, global spending on cybersecurity services is expected to reach $267 billion by 2027, with a significant portion allocated to training and awareness.

However, despite these figures, many organizations still do not effectively prioritize employee education.

Another relevant data point from a Verizon study (Data Breach Investigations Report 2024) highlights that human error remains a key factor in most security breaches. This underscores the critical importance of awareness. Statistics vary, but consistently show that companies with robust awareness programs experience significantly fewer human-factor-related incidents compared to those without.

Speaking of robust awareness programs, I'd like to emphasize the importance of choosing a customized or human-created program over learning platforms that offer ready-to-consume training packages. These have started to proliferate in many companies, and I can't help but think that the "fast-food-ification" of learning is already here. If your employees aren't completing the training courses they've had pending for months, maybe it's because the quality of the content doesn't invite them to want to do it.

Call to awareness action

My message is clear: let's abandon the tactic of fear, negativity, and gloomy words. Instead, let's embrace an approach based on empowerment and education. By fostering a culture of continuous learning, curiosity, and proactivity, we can transform every employee into a cybersecurity advocate, capable of protecting themselves and the organization from digital threats.

What do you think about the role of fear in cybersecurity awareness? How do you believe we can better empower our employees to be our strongest defenders?

Leire Cubo Arce
Cybersecurity Analyst

Quantum Simulation

Quantum Space by María Gutiérrez

In recent years, quantum computing has moved beyond being a purely theoretical concept and has started to find applications in economically strategic sectors. It is particularly efficient at solving complex problems such as the simulation of physical systems, process optimization, machine learning, and cryptography. Its impact across various industries is undeniable, yet its integration into business operations still faces multiple challenges.

Specifically in the context of simulation, while significant hurdles remain—such as quantum noise and errors, scalability, and the need for hybridization with classical methods—it remains one of the most promising applications. Quantum simulation enables the modeling of highly complex problems with an efficiency that classical systems cannot match. A compelling example is the study conducted by Multiverse Computing, a pioneering company in the financial sector, in collaboration with Crédit Agricole. Together, they developed a model based on quantum-inspired neural tensor networks to optimize the pricing of complex financial products.

What problem were they trying to solve? In the world of finance, calculating the fair price of a financial product (known as pricing) is a critical task, especially for derivatives or structured products, whose valuation depends on multiple variables and market scenarios. Traditionally, these calculations are carried out using Monte Carlo simulations, a statistical method that demands enormous computational power and time—especially when precise simulations are needed under various "what-if" market conditions. In the case of Crédit Agricole, the challenge was to find a faster and more efficient way to perform these calculations without compromising accuracy, while also enabling better personalization of pricing based on different clients and market conditions. This is where quantum simulation comes into play.

Multiverse Computing did not use a physical quantum computer, but rather applied a "quantum-inspired" simulation approach—that is, mathematical models that mimic some of the structures and advantages of quantum computing, but are executed on classical computers. In particular, they applied a technique based on quantum neural tensor networks, a type of artificial intelligence architecture that allows highly complex representations to be handled with great efficiency.

Tensor networks originate from quantum physics, where they are used to describe systems with multiple entangled particles. In artificial intelligence, they are adapted to manage large volumes of data with multiple interdependencies—similar to those found in financial markets. In this case, they were applied to a pricing model for financial derivatives, enabling a reduction in the number of required simulations, maintaining high precision in the results, accelerating computation time compared to traditional methods, and performing sensitivity analyses almost in real time.

The impact of the project was significant: the bank was able to improve the efficiency of its pricing system by reducing computational resource usage and increasing its capacity to personalize products. Moreover, this approach supports better decision-making by enabling the simulation of multiple scenarios in much shorter timeframes. This has enormous strategic value in a financial environment where conditions can shift within minutes.

This case demonstrates how quantum simulation using quantum-inspired systems can already transform complex sectors such as finance—without having to wait for fully operational commercial quantum computers.

Emails to Valmont 2.0

Article by David Contel

Pedagogical innovation has been key to the consolidation of the Awareness area and the development of sufficiently imaginative actions that, on the one hand, achieve learning objectives and, on the other, generate strong engagement with user groups accustomed to the constant evolution of content consumption.All too often (and systematically), we fail to critically reflect on the media we use and instead let technological trends and new educational tools dictate our direction by inertia. The result can be the uncritical adoption of a novel format by default, placing less emphasis on what we actually want to communicate.

In this article, we want to encourage reflection on classic communication styles and media—and how, far from being outdated tools, they can be used effectively to support awareness goals.

Let's begin with a question: what are a thread of emails, a string of SMS messages, or posts in a discussion forum? Simply put, letters. And in the history of literature, that's called an epistolary novel.

This is an example of how a classic literary style can be transformed into a powerful awareness tool. We'll leave the conclusions to the reader.

Excerpts from the diary of a Finance CIO

Monday, August 18 – 11:15 AM

Just saw the CEO's Instagram. Looks like he's having a blast skiing in Argentina. I'm going to upload a few things from these past days to my own socials. That photo of the girls holding the sign for my mom—"Tamara and Cayetana love you. Happy birthday, Grandma"—is the sweetest thing I've seen in a while. Once I post it for all my followers, I'll make a TikTok video using the new summer hit by Karol G.

Friday, August 22 – 6:13 PM

I definitely overdid it with the caipirinhas, and the hotel's babysitting service ends at 7:00 PM—just as my wife is getting out of the spa. I down a soda and pop two ibuprofens. Yesterday's posts are a hit. I've got more likes than Leticia Sabater and the waka waka thing. Wait... or was that Shakira? Better make it three ibuprofens. What's that notification? Oh, right. Time for a BeReal pic.

Monday, August 25 – 3:24 PM

We're flying back home in two days. I've been tempted to check my work email. Luckily, Tadeo—the Colombian bartender—has absolutely nailed the mojito recipe. We've become pretty good buddies.

It's hilarious. The anecdotes from his family business—Exportations' Escobar—are great. I'm glad to hear the company pulled through after the tragic death of their CEO in a plane crash. I gave him my email so he can send over some of the pictures he took of us.

Monday, September 1 – 10:32 AM

After two weeks in Copacabana (Brazil) on vacation with the family, I'm back at work. Honestly, I need a vacation from this vacation. Thankfully, in just a month we've got the international corporate conference in Tijuana. My mood dips even further when I open my Outlook inbox. I'm seriously considering asking my assistant to filter out the important emails. I'll deal with them later... after the morning meetings.

Monday, September 1 – 12:32 PM

The third meeting was with the CISO. He presented the updates to our security policies. Now we have to use 12-character passwords and we're not allowed to reuse them. I'll just stick with "Copacaban@2025" until the end of the year—good luck cracking that one. What really annoys me, though, are the new network security controls. Why are they blocking ChatGPT? On a brighter note, we met the new GRC manager. She seemed really competent. I'll schedule a meeting with her ASAP to get a full breakdown of what she does.

Wednesday, September 10 – 10:32 AM

I've changed my corporate email password to "Copacaba@2025" after the meeting with the new GRC manager. She explained her key focus areas and objectives for the new fiscal year. I'll definitely need several more meetings to wrap my head around all of it. But from what I gathered, we need to stay on top of the changes coming from that NIS2 thing. Before I dig deeper into it, I've got an urgent issue: apparently, the head of payments is having a panic attack and tried to strangle himself with the microwave cable.

Wednesday, September 10 – 10:55 AM

No one's walking away from this alive! What a brainless, clueless, clumsy Neanderthal! How could he possibly think it was okay to transfer two million euros?! And to a different account, no less. Doesn't he know we have procedures for that? And the caveman tells me I asked him to do it—from my personal email—and that he even spoke to my lawyer. At this point, I'll be the one needing a lawyer. A criminal one. If he doesn't finish himself off with the microwave cable, I just might do it myself.

Wednesday, September 10 – 1:35 PM

Today, I'm starting to believe in a higher power. The bank called us to double-check the transfer. They found it suspicious we'd send such a large sum to a brand-new account in a Chinese bank. We were able to cancel it in time. We came this close to a full-blown catastrophe. I'm going to wrap up a few things, pop my fifth Diazepam, and head to the hospital to visit the payments manager. When the ambulance picked him up, they were talking about a possible stroke.

Thursday, September 11 – 8:57 AM

We've completed all the incident response actions. The CISO and his team have analyzed the attack phases and prepared the report. They're also developing specific training for high-risk users to improve cyber awareness. If I had known how critical this was, I would've personally sponsored it. In any case, we're all feeling a bit calmer now. I was happy to hear from Tadeo, the Colombian bartender. He sent me a super nice email—he's such a great guy. Though I was sure I'd given him my personal email, not my work one. Anyway, he shared some resort updates and sent over a bunch of pictures. I just saw the link to his personal Drive. I'll go ahead and download them. This day is already looking up!

Excerpts from the diary of a cybercriminal

Tuesday, August 19 – 2:25 PM

I'm continuing social media surveillance on the finance CIO of the target company. Like any man with delusions of grandeur, he's already posted five times on Instagram today, uploaded two TikToks, and made nine Facebook posts. Classic boomer energy. The pics with his daughters, Tamara and Cayetana, confirm he's still throwing money away on that gym membership. Guess he's more of a Cruzcampo investor than a fitness one..

Saturday, August 23 – 11:25 AM

The target keeps posting stuff. That last BeReal selfie with the bartender doesn't give me much, except the clear forecast that he'll need a liver transplant in a few years. It's late today, but tomorrow I'll find out who his health insurer is and sell that info.

Monday, August 28 – 9:25 PM

I've gained access to the target's personal email account. Feeling proud. Didn't even need to run a wordlist. The mail server accepted the password on the third try: TamarayCayetana2025. I'll check later if he's been sending corporate info from there. For Mother Russia.

By the way—who is this Tadeo Escobar sending him pictures of Sofía Vergara?

Monday, September 1 – 12:01 PM

Confirmed. The target has corporate data in his personal email. The most interesting part is about upcoming payments for IT equipment. I've got full details of the contacts involved, what they usually discuss, and even the jokes they crack among themselves.

I need to find out who this Albert Rivera is and what's the deal with his dog Lucas. With all this info, I can put together a solid Business Email Compromise (BEC) attack.

Tuesday, September 9 – 10:48 AM

The BEC attack plan is ready. I'll send the email to the payments manager from the CIO's personal account. To make it more convincing, I'll bring his "personal lawyer" into the thread. If everything goes as planned, this will earn me a nice commission. I've sent the operation brief to my boss—he liked it so much he gave me a bottle of vodka. He said if I pull it off, I get a promotion.

Wednesday, September 10 – 10:48 PM

The attack was a success. The payments manager did exactly what I expected. After receiving the urgent request to change account details and make the immediate transfer—with just the right amount of pressure from the CIO's personal email—he executed it without blinking.

We should receive confirmation of the funds within a few hours. I've already changed the email password to lock him out.

My boss was so happy, he looked like Boris Yeltsin at an afterparty with Bill Clinton.

Wednesday, September 10 – 11:16 PM

While we’re still waiting for the transfer confirmation, I’m passing the time by deciding where to spend my bonus. Sure, Benidorm is always a safe bet for top-tier tourism, but maybe I’ll visit some friends in Hackerville. Romania is just gorgeous in the summer.

Wednesday, September 10 – 3:23 PM

The bank’s controls kicked in, and the target managed to cancel the transfer. I knew it was a risk, but I’m seriously pissed off. I was already daydreaming about buying a seaside apartment in Marina d’Or.

But the real problem is with my superior. He’s convinced the failure was my fault for not planning better for contingencies.

He called me a traitor. Compared the fiasco to Yevgeny Prigozhin’s march on Moscow and threatened to ship me off to a gulag if I didn’t deliver.

Once he calmed down, I explained another plan I’d been working on, and he gave me one last chance. But he made it clear: if I screw this up again, he’ll consider it a betrayal worse than what Joan Garcia did.

So I’m not wasting any more time. Tadeo Escobar and his lovely photos will be my Trojan horse. I’ve prepared a direct link to the ransomware executable, disguised as a personal drive full of vacation pics.

This time, everything will go according to plan.

David Contel
Cybersecurity Senior Consultant

Approach to cybersecurity awareness activities in organizations

Trends by Gerard Marín Raventos

Cybersecurity is not, for most companies and organizations, the primary purpose of their activity or even their existence. However, by now there is no doubt that cybersecurity has become a critical aspect for any organization. Since it is not the main purpose but is necessary and critical, it is essential that both the company and the people within it have internalized a cybersecurity culture.

This implies that cybersecurity awareness activities must be strategically designed, considering that these organizations need to prioritize their focus on their core operations while integrating security as an added value.

To start, it is essential that cybersecurity awareness be approached pragmatically.

Instead of overwhelming employees with complex technical information, activities should be accessible and relevant to their daily functions. For example, brief workshops can be conducted focusing on how to apply secure practices in their daily tasks, such as handling sensitive information or using strong passwords.

Moreover, awareness activities should be interactive and engaging. Using methodologies like gamification, where employees participate in games or simulations related to cybersecurity, can be very effective.

For example, a company could organize a virtual "escape room," where teams must solve cybersecurity puzzles to "escape" a simulated environment. This type of activity is not only entertaining but also promotes teamwork and reinforces practical learning.

It is also crucial that senior management participates in and supports these initiatives. When organizational leaders show commitment to cybersecurity, employees are more likely to take awareness activities seriously.

The saying "young people close their ears to advice but open their eyes to examples" can also apply to adults. Regular communications about the importance of cybersecurity, accompanied by concrete examples—even from within the organization itself—can increase risk perception and the need to act.

Awareness must be continuous and not a one-time event. Implementing a recurring training program, which addresses different aspects of cybersecurity throughout the year, will help keep employees informed and prepared against new threats.

Finally, measuring the effectiveness of these activities is crucial. Conducting surveys or evaluating employee performance in security simulations will allow programs to be adjusted as needed and demonstrate the impact of awareness initiatives in the workplace.

In conclusion, although cybersecurity is not the core business of an organization, it is essential that awareness activities are effectively integrated into the corporate culture. By adopting a practical, interactive, and continuous approach, organizations can strengthen security without diverting attention from their main objectives..

Gerard Marín Raventos
Cybersecurity Consultant

Vulnerabilities

Critical Vulnerability Found in Sudo

Date: June 30, 2025
CVE: CVE-2025-32463

CVSS: 9.3

CRITICAL

Description

This vulnerability, identified as CVE-2025-32463, refers to the discovery of a design flaw that allows an attacker to invoke Sudo with the -R or --chroot option, exploiting the path resolution before the correct evaluation of permissions. This enables loading a malicious /etc/nsswitch.conf file that in turn points to arbitrary shared libraries, leading to the execution of malicious code as root.

This flaw allows privilege escalation on the system and execution of code as root, even from user accounts not listed in the sudoers file.

Solution

There are no official patches that fix this flaw yet, but only certain versions of Sudo are affected. It is recommended to use the following versions:

- Sudo 1.9.17p1 or later

Additionally, it is advised to disable sudo rules that allow the use of the -R or --chroot options in environments where they are not necessary, or temporarily until the update is applied. It is also recommended to restrict execution permissions of files from directories such as /tmp or /var/tmp.

Affected Products

This critical vulnerability affects several sudo products, including the following:

- Sudo (from 1.9.14 to 1.9.17)
- Sudo (from 1.8.8 to 1.8.32)

References

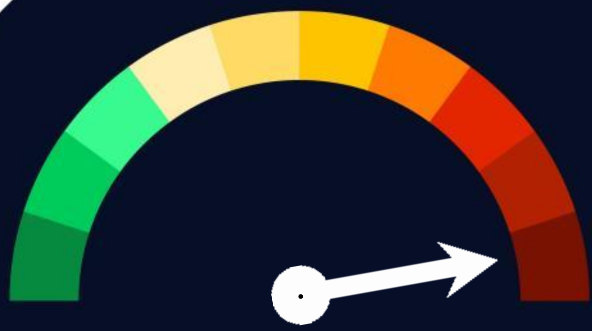
- nvd.nist.gov
- www.incibe.es
- access.redhat.com
- thehackernews.com
- thehackernews.com

TLP:WHITE

Vulnerabilities

Critical severity vulnerability in Chrome

Date: July 2,2025
CVEs: CVE-2025-34090



CVSS: 9.3

CRITICAL

Description

The vulnerability CVE-2025-34090 affects Google Chrome and involves a weakness in cookie encryption through AppBound.

A local attacker can carry out a COM hijacking (Windows Component Object Model hijack) to force Chrome to use the user's DPAPI instead of AppBound, which is a less secure encryption method.

Once the attacker manages to downgrade the encryption, they can perform a Padding Oracle attack, exploiting system error messages during data decryption. This allows them to decrypt encrypted cookies byte by byte, without elevated privileges, and gain access to active web sessions.

Solution

Currently, the CVE-2025-34090 vulnerability in Google Chrome does not have an official patch available.

Therefore, it is essential to take precautions to minimize risks, such as restricting access to CLSID keys in the Windows Registry to prevent COM hijacking attacks.

Affected Products

This critical vulnerability affects:

- Google Chrome versions earlier than 129.
- Other Chromium-based browsers that use similar cookie encryption mechanisms.

References

- cyberark.com
- nvd.nist.gov

Patches

Citrix patches a critical vulnerability affecting NetScaler ADC and NetScaler Gateway

Date: June 25, 2025
CVE: CVE-2025-5777

Critical

Description

The CitrixBleed 2 vulnerability (CVE-2025-5777) affects Citrix NetScaler ADC and Gateway devices, allowing attackers to retrieve memory contents by sending malformed POST requests during login. CitrixBleed 2 can be exploited against configuration utilities used by administrators and to steal session tokens.

According to researchers, each request leaks 127 bytes, enabling attackers to perform repeated HTTP requests to extract additional memory content until they find the data they are seeking.

Citrix has stated that the vulnerability has not been exploited, although there are reports indicating otherwise.

Solution

Citrix recommends in its security bulletin that customers promptly install the updated fixed versions of their NetScaler ADC and NetScaler Gateway products.

Additionally, Citrix advises terminating all active ICA and PCoIP sessions and reviewing existing sessions for any suspicious activity.

Affected Products

- NetScaler ADC and NetScaler Gateway 13.1 (versions prior to 13.1-58.32), 14.1 (versions prior to 14.1-43.56)
- NetScaler ADC 12.1-FIPS (versions prior to 12.1-55.328-FIPS), 13.1-FIPS and NDcPP (versions prior to 13.1-37.235)

References

- netscaler.com
- bleepingcomputer.com
- horizon3.ai

TLP:WHITE

Microsoft July Security Patches to Fix 130 Vulnerabilities

Date: July 9, 2025
CVE: CVE-2025-47981 and 129 more

Critical

Description

Microsoft's July 2025 patch update addresses 130 vulnerabilities, of which 10 are considered critical. The most relevant vulnerabilities identified are:

- CVE-2025-47981 (CVSS 9.8): A critical vulnerability in SPNEGO/NEGOEX that could allow remote code execution (RCE) without user interaction, affecting Windows versions with a certain Group Policy Object (GPO) enabled by default.
- CVE-2025-49719 (CVSS 7.5): A vulnerability in SQL Server that allows access to sensitive information without prior authentication. This vulnerability was publicly disclosed before the patch release and has a publicly available proof of concept (PoC).

Also noteworthy is the following vulnerability:

- CVE-2025-49735 (CVSS 8.8): A vulnerability in Kerberos (Key Policy Service - KPSSVC) that could allow an attacker to execute remote code on the affected system.

According to Microsoft, these vulnerabilities have not been actively exploited.

Affected Products

These vulnerabilities impact a wide range of Microsoft products. To see all affected products, please refer to the following link:

- msrc.microsoft.com

Solution

Microsoft recommends applying the security patch released to address the detected vulnerabilities.

References

- msrc.microsoft.com
- thehackernews.com

TLP:WHITE

Events

DEF CON 33
7 - 10 August

The event will take place from August 7 to 10, 2025, at the Las Vegas Convention Center – West Hall (USA), and promises to be an intense, diverse, and deeply technical experience. This event is not just for hackers: it is also ideal for researchers, defenders, developers, analysts, and digital enthusiasts. This year's theme, "Access Everywhere," focuses on making information and services accessible to everyone, regardless of device, location, or abilities.
The event consists of:

- Themed Villages: dedicated spaces for specific areas like IoT, biohacking, networking, hardware, artificial intelligence, and more.
- Talks and Keynotes: presentations from global experts on vulnerabilities, attack techniques, defense, and forensic analysis.
- CTF Competitions (Capture The Flag): technical challenges for teams worldwide, from beginners to professionals.
- Demo Labs: where creators showcase hacking, defense, and analysis tools live.
- Workshops: hands-on 4-hour sessions on topics like reversing, pentesting, OSINT, and more.
- Social events and meet-ups: from hacker karaoke to ham radio groups, themed parties, and informal networking.

Link

International Conference on computer Science, Programming and Security ICCSPS
14 - 15 August

The goal is to bring together academics, researchers, and industry professionals to share experiences and advancements in areas such as computer science, secure programming, data protection, and cybersecurity. The event will be held in Barcelona (Spain) on August 14 and 15.

Link

Bsides Bournemouth
16 August

Each BSides is a community-driven framework designed to create events by and for members of the information security community. It creates opportunities for people to present and engage in an intimate environment that fosters collaboration.

It is an intense event featuring discussions, demonstrations, and participant interaction.

Link

GRC Conference 2025
18 – 20 August

ISACA and The IIA will gather leading minds in Governance, Risk, and Compliance (GRC) in New York (USA) to provide dedicated professionals with world-class content, innovative ideas, and practical guidance.

Attendees will gain critical insights and hands-on knowledge across a variety of topics designed to address current challenges and opportunities.

This year’s sessions are carefully selected to empower professionals with practical tools, innovative strategies, and forward-looking ideas to excel in their roles and advance their organizations.

Link

Resources

➢ Vastav AI: Deepfake and Disinformation Detection

Vastav AI offers a powerful solution using forensic machine learning and metadata analysis. It examines visual and audio content for signs of manipulation. Its intuitive heatmaps and confidence scores enable researchers, journalists, and analysts to quickly identify altered media.

Link

➢ Vectra AI: Network and Cloud Attack Signal Intelligence

Vectra delivers continuous AI-powered monitoring to detect hidden attacker behaviors, such as lateral movement, privilege abuse, and command-and-control activities before damage occurs. Its true strength lies in reducing alert fatigue by prioritizing high-risk, genuine threats.

Link

➢ PentestGPT: AI-Powered Penetration Testing Assistant

PentestGPT is an AI-driven penetration testing assistant based on GPT models that helps ethical hackers optimize their workflow. Instead of spending hours on manual reconnaissance or report writing, users can delegate these tasks to PentestGPT.

It offers guided scans, generates structured vulnerability reports, and even creates custom scripts tailored to the engagement.

Perfect for solo pentesters, bug hunters, and red teams looking to speed up common, repetitive tasks without compromising quality or thoroughness.

Link

Subscribe to RADAR

Powered by the cybersecurity NTT DATA team

es.nttdata.com