Issue 109 | December 2025

NTT DATA

Radar

The Cybersecurity Magazine

When hacking evolves faster than code

By Jose Carlos Moral

Software development is no longer a race to launch faster, but to launch safer. In this new paradigm of continuous improvement, security has stopped being the final checkpoint before deployment and has become the thread that connects every stage of development.

We live in an ecosystem where attacks evolve as fast as the code trying to stop them.

Today, cybercriminals no longer hide in dark basements — they're in AI labs, private forums, and often inside the very companies they're trying to protect.

New hacking techniques — AI-powered phishing, prompt injection, supply chain exploits, or operational deepfakes — are redefining the rules of the game.

It's no longer enough to think about firewalls or antivirus; the challenge now is to stay ahead and build software that thinks like an attacker before a real one does.

Shift Left: Secure code is born from the first line

In secure development, "shift left" is no longer an aspirational concept — it's a necessity. Integrating security into every phase of the Software Development Life Cycle (SDLC) not only reduces remediation costs but also minimizes the attack surface before the product ever goes live.

Automating audits, using SAST and DAST, incorporating threat modeling, and reviewing third-party dependencies should be as routine as committing code.

Because a single flaw in a dependency can become the next global breach.

SolarWinds, Log4Shell, and XZ Utils are recent reminders that the digital supply chain is only as strong as its most forgotten link.

The Human Factor: From Weak Link to Smart Shield

No matter how advanced detection techniques become, social engineering remains the most effective entry point.

And here lies the big shift of this new era: user education. It's not about turning everyone into cybersecurity experts, but about transforming digital culture.

The focus should be on enabling a developer to recognize when code might be vulnerable, or helping an employee pause before clicking a link that doesn't look quite right.

The Future of Hacking Is Collaborative

Ethical hacking, bug bounty programs, and collaboration between white-hat communities and companies are driving a new mindset: that of shared defense.

In a world where cyberattacks have become an industry, only a collective response can stand against them. Security is no longer just a layer — it's an attitude.

And like every attitude, it begins with how we think about software from the very start.

Jose Carlos Moral
Cybersecurity Manager – Security Architecture

Closing 2025

Cyber chronicle by Joel Perez

In the second half of 2025, the cybersecurity landscape has entered a phase of accelerated mutation. The old recipes of mass phishing or basic ransomware no longer suffice; adversaries are refining new hacking techniques —more sophisticated, multidimensional, and dangerous— that demand heightened vigilance and an urgent response.

AI, Automation, and Deepfakes: The Silent Weapon

Recent reports indicate that AI-powered attacks are no longer futuristic — they're being deployed at scale. According to Check Point Software, by 2025 "states and criminal organizations are using AI-based tactics, including disinformation campaigns and disruptive malware." For example:

- Generative models creating phishing emails almost indistinguishable from legitimate ones.
- Deepfakes with voice or video impersonating executives or employees to gain privileged access.
- Automated intrusion processes that drastically shorten the time between discovery and exploitation.

These techniques have turned the "traditional hacker" into something closer to a digital orchestrator: instead of sending five mass emails, dozens of AI-generated, hyper-personalized attacks are crafted, each tailored to its specific target..

Multi-Platform, Supply Chain, and Malware-Free Attacks

Tactics are also diversifying toward more complex vectors than ever before. For instance, experts highlight the rise of:

- Supply chain attacks: compromising a third-party element to reach the ultimate target.
- Multi-platform attacks: targeting multiple operating systems (Windows, Linux, mobile, and even cloud environments) within the same campaign.
- Fileless techniques: operating through legitimate system processes, RAM, or cloud services — moving stealthily without leaving traditional malware traces.

This means that many traditional defenses — antivirus, firewalls, malware signatures— are no longer sufficient on their own.

Triple Extortion, Infostealers, and the Cloud Perimeter Under Fire

The evolution of ransomware also defines this new era of hacking: it's no longer just about disk encryption, but about data theft, publication, social pressure, and multiple layers of extortion. One of the key techniques for 2025 is triple extortion (theft + encryption + public exposure), often combined with deepfakes and targeted attacks.

At the same time, so-called infostealers — programs designed to steal sensitive information— have multiplied, acting as entry points to the full attack chain.

Meanwhile, the expansion of cloud environments, IoT, and edge devices has opened up new fronts: attackers no longer break in through the typical office network, but through peripheral devices, SaaS services, vulnerable containers, and microservices.

Persistent Threats, Collaboration Between Actors, and Rapid Reuse

Adversaries —whether criminal groups, hacktivists, or nation-states— are also evolving structurally:

- Collaboration between APTs (Advanced Persistent Threat groups) and criminal gangs, merging espionage motives with financial gain.
- Rapid reuse cycles, with modular, ready-to-use toolkits and fast adaptations that allow a technique discovered today to become widespread within weeks.

The element of surprise has become routine: fewer "noisy" attacks and more stealthy, long-term operations that demand proactive rather than reactive detection.

What to Do: Countermeasures to Stay Ahead

Given this landscape, defensive strategies must evolve:

- Adopt continuous monitoring and behavioral analysis, not just signature-based detection.
- Integrate AI and automation into defense — if attackers use AI, defenders must rely on artificial intelligence too.
- Segment environments and harden the perimeter, but also secure the inside — the cloud, endpoints, and third-party services.
- Prepare advanced simulations and rapid-response exercises, and assume that an "incident" won't be an isolated event but a prolonged campaign.
- Train personnel to recognize deepfakes, ultra-personalized spear-phishing, and attacks unfolding outside traditional email channels.

Conclusion

We are entering a new era of hacking — one defined by speed, automation, AI-driven tactics, and increasingly complex attack vectors that demand a complete rethink of both offense and defense.

The techniques described are no longer "what's coming next"; they are happening here and now. Cybersecurity professionals face a dynamic, multidimensional, and demanding battlefield — one that rewards foresight as much as resilience.

Mic-E-Mouse: when the mouse becomes a microphone

Article by Rodrigo Rey and Alberto Agra

In a world where artificial intelligence (AI) is advancing faster than security measures, every new discovery in cybersecurity forces us to rethink the boundaries of technology. The latest study, known as Mic-E-Mouse, has uncovered an unexpected vulnerability: computer mouse motion sensors can be exploited to capture ambient sounds, effectively turning them into improvised microphones. This revelation not only presents a technical challenge but also raises an ethical debate about the risks of human ingenuity in the age of AI.

The research, published in mid-September 2025 by a group of cybersecurity experts from several universities, had a simple yet unsettling goal: to explore whether the optical and motion sensors found in common computer mice could record the minute vibrations caused by sound waves.

These sensors, originally designed to detect surface movements, capture light changes at extremely high speeds — in some models, up to 30,000 times per second. The researchers realized that, under certain conditions, these fluctuations could reflect vibrations produced by nearby voices or sounds.

The finding quickly spread through specialized media such as TechSpot, Kaspersky, GBHackers, and The Indian Express, surprising the tech community and serving as a reminder that cyber threats don't always come from malicious software — sometimes, they emerge from the physical devices themselves.

The attack described by the researchers is based on a simple physical principle: every sound generates mechanical vibrations on nearby surfaces. When a high-resolution optical mouse rests on a desk, those microscopic vibrations can alter the light reflection the sensor uses to calculate movement.

The scientists developed an AI model capable of analyzing the data captured by the sensor — seemingly just movement coordinates — and filtering it to reconstruct frequency patterns associated with human sounds. With sufficient training, the neural network was able to identify fragments of speech and recognize specific words, achieving surprising accuracy under controlled conditions.

The attack, dubbed Mic-E-Mouse, doesn't require physical access to the computer's microphone — or even to any audio components. It would be enough to compromise the mouse's firmware or intercept the movement data transmitted to the computer. While the process remains experimental and its practical execution complex, it proves that even the most ordinary peripherals can be turned into espionage tools.

The Mic-E-Mouse experiment is not merely a technical demonstration — it's a warning about the future of digital privacy. The ability to turn a mouse into a listening device shows just how far AI can reinterpret the physical boundaries of technology.

Although the attack does not yet represent a large-scale threat, its very existence reminds us that security must be conceived as an integrated system, where every component — no matter how trivial it may seem — could become an open door to risk.

Ultimately, this study invites us to reflect on our relationship with technology. It's not just about building smarter machines, but about ensuring that their intelligence doesn't turn against us..

Rodrigo Rey
Cybersecurity Lead Architect

Alberto Agra
Cybersecurity Expert Architect

Quantum Awareness

Quatum Space by María Gutiérrez

We close this 2025 Year of Quantum Science and Technologies with the conviction that the quantum world is no longer a promise — it's the present. In recent months, we've seen practical applications emerge in healthcare, energy, logistics, finance, and communications. Quantum physics no longer lives solely in formulas, laboratories, or research centers; it's beginning to weave itself into our everyday lives. In fact, it may have always been there — particularly within our own brains.

Quantum phenomena such as superposition, entanglement, and coherence could play an essential role in the processes that give rise to subjective experience — that mysterious quality that makes us "be" and "feel." We're not talking merely about information or neural processing, but about the deepest substrate of conscious mind itself. Could this be what we call consciousness?

For decades, scientists believed the brain, operating at body temperature, was far too warm and noisy an environment to sustain quantum coherence. However, in recent years, experimental results have reignited the debate. In quantum biology, coherence has been observed in living systems — such as photosynthesis and the navigation abilities of certain birds — showing that life can harness quantum effects even under "non-ideal" conditions.

The idea began to take shape in the 1990s, when physicist Roger Penrose and anesthesiologist Stuart Hameroff proposed the Orch-OR (Orchestrated Objective Reduction) theory. According to their hypothesis, consciousness arises from quantum processes within microtubules — structures of the cell's cytoskeleton — that allow superposition states in the brain. These states would collapse in an orchestrated manner, producing discrete moments of consciousness..

This has sparked a growing field of research that some call quantum neurobiology, which explores the limits of decoherence in neural structures and the possible interaction between quantum processes and cognition. Although we are still far from a solid demonstration, the mere possibility is reshaping how we understand the mind.

These ideas border on the metaphysical, yet they also pose an empirical challenge: can we design experiments capable of distinguishing a classical brain from a "quantum" one? Some projects, still in the conceptual phase, are attempting to detect signatures of entanglement in neural networks or non-classical correlations in brain activity.

The technical difficulty is immense — but the potential impact would be revolutionary. At a time when intelligence no longer seems to define us as humans (AI surpasses us in memory, capacity, and speed, though it still requires far more energy to learn…), the search for what truly makes us unique leads us back to consciousness.

Could consciousness itself be what sets us apart? But what if it turns out to be a matter of complexity, of quantum state collapse? Could quantum computing, designed to resolve complex problems, one day endow AI with consciousness — meaning that even this might not be what makes us "unique" or "different"?

Quantum consciousness is not, as of today, a proven theory — but rather an invitation to think. And that very act of thinking, straddling physics, biology, and philosophy, will undoubtedly be one of the great arenas of scientific debate in the coming decades.

The year 2025 may be ending — but the quantum debate is only just beginning.

EDR Evasion: The New Frontier of Offensive Security

Trends by Jesús Murciano

Throughout 2025, one trend has captured the attention of cybersecurity researchers: EDR (Endpoint Detection & Response) evasion. These platforms — the first line of defense against advanced threats — are being analyzed both by researchers and by attackers seeking to bypass their detection and response mechanisms.The rise of tools like EDRFreeze marks the beginning of a new stage in the ongoing arms race between offense and defense. It's no longer just about hiding malware — it's about temporarily neutralizing the guardian that protects the systems.

What Does This Technique Involve?

Until recently, the most common strategies for evading EDRs involved using vulnerable drivers — a method known as BYOVD (Bring Your Own Vulnerable Driver) — which granted kernel-level privileges to disable security services. However, this approach required advanced access and often left detectable traces.

The paradigm shift has come with methods like EDRFreeze, which operate entirely in user mode. By leveraging legitimate operating system mechanisms such as Windows Error Reporting (WER), these tools can suspend or "freeze" security processes without exploiting kernel vulnerabilities or loading signed drivers.

In practice, this means an attacker can pause EDR monitoring long enough to execute malicious code, move laterally, or exfiltrate data — all without triggering immediate alerts.

Why Is This Trend So Effective?

The effectiveness of this technique lies in its low profile and its use of legitimate system components. By relying on native Windows processes and executing with standard permissions, attackers dramatically reduce the likelihood of detection by traditional defenses.

This approach aligns with the "living off the land" philosophy — the evolution of evasion tactics that emphasize discreet use of the system's own resources rather than external tools. It's a subtle yet powerful reminder that, in modern cybersecurity, the most dangerous attacks often hide in plain sight.

Moreover, these tools eliminate the need for deep kernel-level knowledge, broadening their adoption among less sophisticated actors. At the same time, research within offensive security communities has accelerated the release of proofs of concept and scripts that replicate process-suspension behavior — suggesting that even attackers with limited technical expertise will soon be able to carry out increasingly advanced attacks.

Conclusion

EDR evasion marks a significant evolution in attacker tactics and forces defenders to adapt quickly. Protecting the defense mechanisms themselves has become a strategic priority. Organizations must strengthen process integrity controls, apply blocklists for vulnerable drivers, monitor anomalous use of system services, and — most importantly — detect "EDR silences" — the periods when telemetry stops reporting — as potential indicators of compromise.

In an increasingly sophisticated environment, where the goal is no longer just to breach the system but to disable those who defend it, the resilience of defensive mechanisms will be the true differentiator.

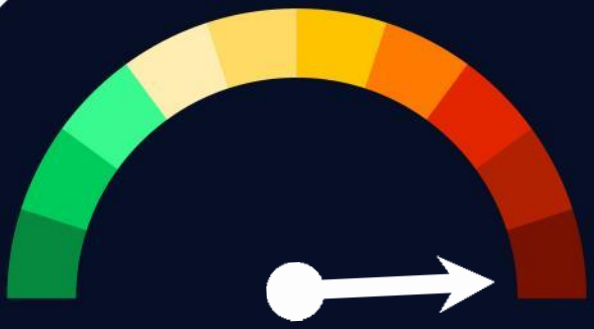
The race to "freeze the EDR" has only just begun.

Jesús Murciano
Cybersecurity Analist

Vulnerabilities

Critical vulnerability in React Native Metro CLI

Date: November 3, 2025
CVE: CVE-2025-11953



CVSS: 9.8

CRITICAL

Description

The critical vulnerability CVE-2025-11953 allows remote attackers to execute arbitrary code on developers' machines running the React Native Metro development server.

The root cause of the vulnerability lies in the server's failure to properly validate the lineNumber and file parameters. On Windows, the server invokes the editor using Node.js's child_process.spawn function and passes the file and line as arguments; if lineNumber includes shell metacharacters, cmd.exe interprets them and enables the execution of arbitrary commands.No authentication is required, and commands can be executed remotely if the attacker can access the server port (default: 8081).

Solution

The following steps will mitigate the CVE-2025-11953 vulnerability:

- Update @react-native-community/cli-server-api to version 20.0.0 or later, which includes the fix for this vulnerability.
- To enhance security—or if updating is not possible—configure the development server to bind explicitly to the localhost interface by including the option --host 127.0.0.1.

Products Affected

This critical vulnerability affects all versions prior to the commit that fixes the improper input parameter validation, resolved in React Native CLI, specifically in the Metro Development Server component for versions earlier than 20.0.0. Exploitation of the vulnerability is particularly severe on Windows systems.

References

- nvd.nist.gov
- jfrog.com

TLP:WHITE

Vulnerabilities

Critical vulnerabilities in Cisco's UCCX product

Date: November 5, 2025
CVE: CVE-2025-20354 and 1 more

CVSS: 9.8

CRITICAL

Description

Cisco has disclosed two critical vulnerabilities affecting its Unified Contact Center Express (UCCX) product.

The vulnerability CVE-2025-20354 could allow a remote, unauthenticated attacker to upload malicious files and execute code with administrator privileges. This issue is caused by a failure in the UCCX authentication mechanism.

Meanwhile, the vulnerability CVE-2025-20358 could enable an attacker to bypass authentication and gain administrative access. This flaw results from an authentication failure between the CCX Editor component and the UCCX server.

Solution

The vendor has released a patch addressing the vulnerability. Therefore, it is strongly recommended to update immediately to one of the following versions:

- 12.5 SU3 ES07
- 15.0 ES01

Affected Products

The vulnerability affects all UCCX installations, regardless of the configuration in place.

References

- sec.cloudapps.cisco.com

TLP:WHITE

ShopLentor for WordPress patches a critical vulnerability

Date: November 4, 2025
CVE: CVE-2025-12493

Critical

Description

ShopLentor (formerly known as WooLentor) is a popular WordPress plugin that integrates WooCommerce with the Elementor and Gutenberg page builders. With millions of downloads and a large active user base, it plays a key role in the WordPress e-commerce ecosystem.

Recently, the CVE-2025-12493 vulnerability was identified — a Local File Inclusion (LFI) flaw affecting all versions up to 3.2.5. The issue stems from the load_template function, which fails to properly validate user-supplied file paths, allowing sequences such as ../ to access internal server files like wp-config.php.

Classified as CWE-22, this vulnerability could lead to exposure of sensitive information or even remote code execution, without requiring authentication — significantly increasing its severity. As of now, no proof-of-concept or exploit code has been published, but it is strongly recommended to update the plugin immediately to a patched version.

Affected Products

The affected plugin is ShopLentor – WooCommerce Builder for Elementor and Gutenberg. The vulnerability impacts all versions up to and including 3.2.5, and can be exploited on any WordPress site running a vulnerable version of the plugin.

Solution

Update the ShopLentor WordPress plugin to the latest version (3.2.6 or higher).If immediate updating is not possible, it is recommended to disable the plugin and implement specific WAF (Web Application Firewall) rules to block potential exploitation attempts.

References

- nvd.nist.gov
- wordfence.com

Google fixes vulnerability in Chrome

Date: November 5, 2025
CVE: CVE-2025-12725, CVE-2025-12727 and 3 more

High

Description

Google recently released a security patch addressing five vulnerabilities affecting various components of the Chrome browser, including WebGPU, JavaScript V8, and Omnibox. These vulnerabilities could potentially allow remote code execution.

The most relevant patched vulnerabilities are:

- CVE-2025-12725 (CVSS 8.8): A vulnerability that could allow an attacker to execute code remotely due to an Out-of-Bounds write flaw.
- CVE-2025-12727 (CVSS 8.8): This vulnerability could enable remote code execution through a flaw in the JavaScript V8 engine.

Affected products

The affected product versions are as follows:

- Windows: Versions prior to 142.0.7444.134/.13
- 5macOS: Versions prior to 142.0.7444.135
- Linux: Versions prior to 142.0.7444.134

Solution

The manufacturer recommends updating to the following versions:

- 142.0.7444.134/.135 on Windows.
- 142.0.7444.135 on macOS.
- 142.0.7444.134 on Linux.

References

- chromereleases.googleblog.com
- cybersecuritynews.com

Events

SANS CyberThreat Summit 2025
3 - 4 December

The iconic Stamford Bridge stadium in London will host a two-day conference designed specifically for cybersecurity professionals — both offensive and defensive. Organized by the SANS Institute, this event offers a deep technical immersion, allowing attendees to explore the latest tactics, tools, and real-world attack and defense cases in a high-level environment.Perfect for those on the path to becoming cybersecurity managers: two intensive days, top-tier networking, and the trusted SANS legacy guaranteeing quality.

Link

Black Hat Europe 2025
8 – 11 December

London once again becomes the European epicenter of cybersecurity with this high-impact event. Held at ExCeL London, it features everything from specialized two- and four-day training sessions to main conference briefings on the 10th and 11th, where cutting-edge research is unveiled. Attendees can also enjoy open-source tool demonstrations (“Arsenal”), exhibition halls, and extensive professional networking opportunities.

Link

León Cybersecurity Conference
20 December

On Saturday, December 20, 2025, at Cañada de Mariches #3435 in León de los Aldama (Guanajuato, Mexico), this one-day conference will take place — an event that marks a true turning point for the Bajío region in the field of digital security.

Bringing together national and international voices, it aims to empower both individuals and organizations to face the challenges of the digital landscape, with a strong focus on education, upskilling, and inspiration.
Link

Resources

➢ AdaptixC2

Adaptix is an extensible post-exploitation and adversary emulation framework designed for penetration testers. The Adaptix server is written in Golang, providing flexibility to the operator, while the GUI client is built in C++ using Qt, making it compatible with Linux, Windows, and macOS operating systems.

Link

➢ LLM Red Teaming Framework

DeepTeam integrates the latest research to simulate adversarial attacks using state-of-the-art (SOTA) techniques such as jailbreaking and command injection, aiming to detect vulnerabilities like bias and personally identifiable information (PII) leaks that might otherwise go unnoticed. Once these vulnerabilities are identified, DeepTeam provides mitigation measures to prevent issues in production environments.

Link

➢ DumpGuard

Darktrace has evolved its platform to detect threats by learning the normal behavior of the network, without relying on known attack signatures. Its autonomous response capability, Antigena, can contain attacks in a targeted way without disrupting business operations.

The platform leverages behavioral analytics to identify high-risk anomalies, including sophisticated AI-driven threats, while building unique models tailored to each organization's digital environment.

Link 1

Link 2

Subscribe to RADAR

Powered by the cybersecurity NTT DATA team

es.nttdata.com