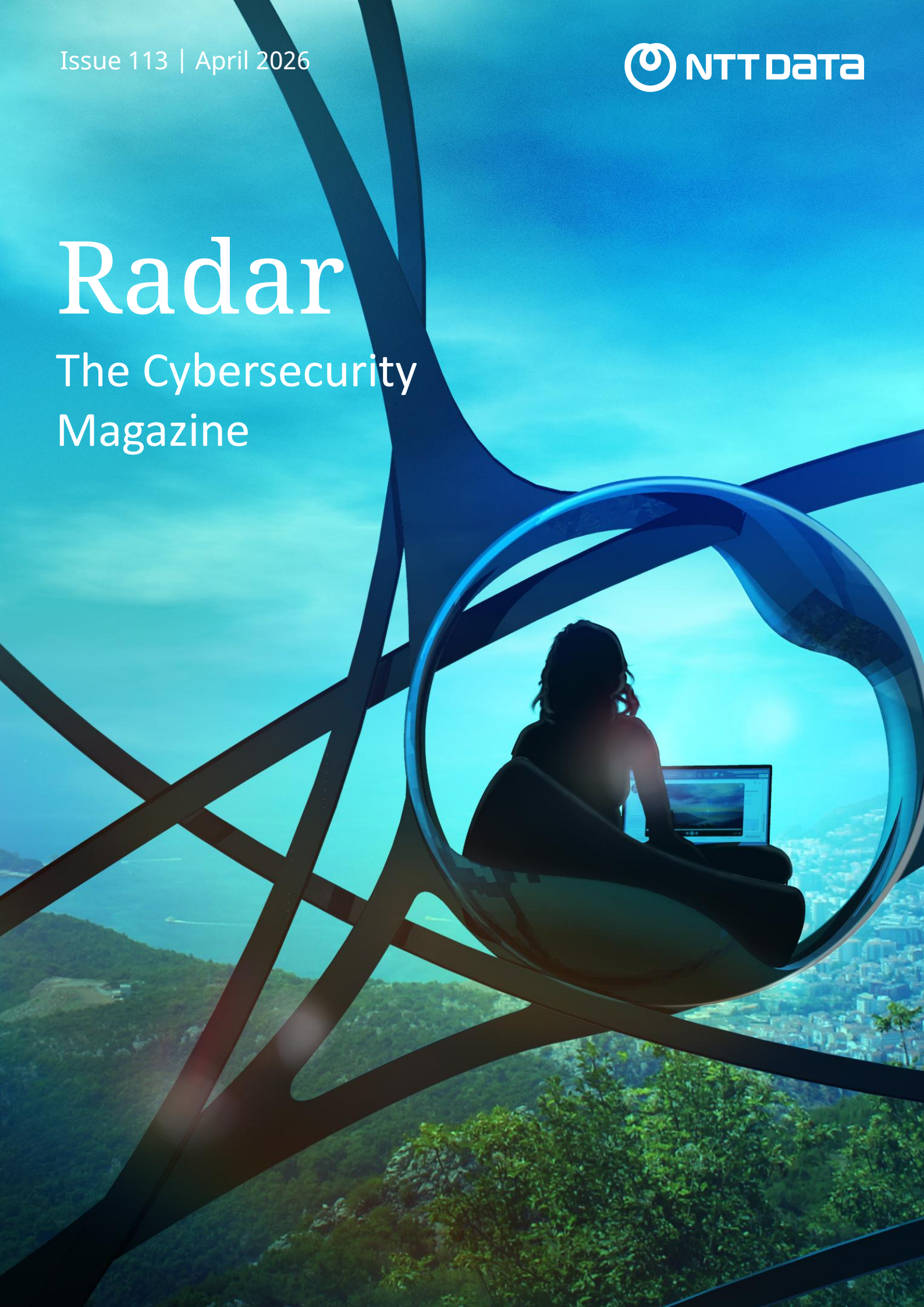
Issue 113 | April 2026

NTT DATA

Radar

The Cybersecurity Magazine



AI and Cyber Security: The New Battle Between Algorithms

By Pedro Felipe del Jesús Canto Vela

We have never had so much technological capacity to protect ourselves, nor so much to attack. Artificial intelligence has burst onto the cyber security landscape as a turning point, redefining the balance between defense and risk. The very algorithms that detect threats in milliseconds can also be used to launch faster, more precise and more difficult to trace attacks. Automation is no longer just a competitive advantage; it is the new battlefield.

For years, security was based on strengthening infrastructures and improving incident response. However, artificial intelligence, particularly generative AI and advanced machine learning models, has transformed the landscape. We are not only facing more sophisticated threats, but also an environment where the speed of adaptation makes the difference. AI accelerates attack and enhances defense, forcing organizations to rethink their strategy beyond simple technological adoption.

In the offensive domain, artificial intelligence has lowered the barrier to entry for cybercrime. Phishing campaigns are personalized in real time, deepfakes enable credible impersonation, and malware adapts dynamically to evade controls. Social engineering is supported by models capable of generating convincing and contextualized messages. But the greatest shift is not only sophistication, it is speed. Attackers can test variants and adjust tactics within hours, while many organizations still operate with processes designed for a slower context.

The democratization of these technologies expands the threat surface and complicates attribution. In an environment without a defined perimeter, with cloud infrastructures and digital supply chains, new risks emerge such as data exposure in generative models, prompt injection, or the poisoning of models. Risk no longer lies solely in infrastructure, but also in the algorithms and the data that feed them.

However, AI is also an essential pillar of modern defense. It enables the analysis of large volumes of information in real time, the detection of anomalies, the prioritization of alerts, and the automation of responses, reducing reaction times. Predictive analysis helps anticipate threats before they become critical incidents, strengthening a more proactive posture.

The key does not lie in technology alone, but in its integration within a robust framework of governance and risk management. Artificial intelligence amplifies capabilities, but it does not replace strategy or human judgement. Without proper oversight and controls, it can lead to misaligned decisions or a false sense of security.

In the age of automation, the real advantage does not lie in adopting AI faster than attackers, but in integrating it deliberately within a model of resilience. Because even as algorithms accelerate the game, the responsibility for protecting the future remains deeply human

Pedro Felipe del Jesús Canto Vela
Cybersecurity Expert Analyst

When artificial intelligence learns to deceive and to operate

Cyber Chronicle by Juan Pablo Camperos

Between 2024 and early 2026, artificial intelligence has ceased to be merely an efficiency tool and has become an operational risk factor. Not because it introduces entirely new threats, but because it amplifies existing ones at a speed that organizations still cannot govern.

One of the most visible examples of this evolution is the use of deepfakes in corporate fraud. In Asia, an employee joined a video call with what appeared to be executives from their organization. The voices, gestures, and context were consistent. The instruction was direct: execute urgent transfers. There was no technical exploitation or malware, only misused trust. Visual identity was no longer sufficient.

A similar case in Singapore reinforced this trend. A chief financial officer was persuaded to transfer a substantial sum after interacting with an executive meeting entirely generated by AI. The deception was only detected when the attackers attempted to escalate the operation. In both scenarios, the technology did not attack the system, it attacked perception.

This shift redefines the entry point. Social engineering no longer depends exclusively on human persuasion, but on the ability to replicate identities with precision. The question is no longer whether the message is credible, but whether there is a process in place to question it.

In parallel, another front began to show more structural risks. Microsoft initiated legal action against a group that used compromised credentials to access generative artificial intelligence services. The objective was not to steal information, but to exploit the infrastructure to generate malicious content and commercialize its use. The problem was not in the model, but in access control.

At the same time, the AI supply chain began to show failures similar to those seen in traditional software. Recent research identified malicious models published in open repositories, designed to execute code when integrated into development environments. Models are no longer passive data; they are becoming active components within the system.

Added to this is an element that many organizations still underestimate: information management. In South Korea, authorities detected that an AI platform had transferred user data and prompt content without consent. This incident revealed a critical issue: prompts contain business context, decisions, and sensitive information. Treating them as disposable text is, in practice, a data leak.

However, the most relevant turning point appears when these patterns reach operations. At Amazon, a series of incidents during 2026 showed how the use of coding assistants and AI based automation can impact production systems. Changes executed at high speed, without sufficient validation and with weak controls, led to disruptions and significant operational losses.

This type of situation marks the convergence between IT and OT. When artificial intelligence stops assisting and begins to influence execution, the impact is no longer just digital. An error can escalate from a configuration to affecting the full continuity of a service.

And this phenomenon is not limited to digital environments. In drinking water systems, unauthorized access has been documented where operational parameters were altered. In the oil and gas sector, manipulation of sensors has generated false alarms and incorrect decisions. In these cases, AI is not the direct origin of the attack, but it is an accelerator that reduces the effort required to reach that point.

Even more concerning is that access is no longer always achieved by exploiting systems. Recent cases show how actors use AI to build credible identities and pass through hiring processes. Once inside, the attacker no longer needs vulnerabilities, they have legitimate access. In environments where industrial systems are connected or remotely managed, this type of infiltration represents a structural risk.

Taken together, these incidents show a clear evolution. Identity is no longer reliable based on appearance, access remains the weakest point, the supply chain extends to models, and automation amplifies any error. AI does not break systems, it accelerates their failures.

When these patterns reach operational environments, the nature of the impact changes. A fraud can disrupt payments to critical suppliers, a compromised credential can open access to industrial systems, and a poorly controlled automated change can affect entire production processes. Cybersecurity stops being a technical issue and becomes a matter of continuity.

The response is not to limit the use of artificial intelligence, but to govern it. The organizations that are moving forward are not those that invest the most in AI, but those that establish clear controls over its use and, above all, over its impact.

Because in this new landscape, the question is no longer whether AI can be used in an attack, but whether organizations are prepared to operate with it without losing control.

Juan Pablo Camperos
Cybersecurity Expert Architect

Beyond the Illusion: Disinformation and Deepfakes in the Age of AI

Article by Prakash Narayanamoorthy and Ben Colman*

This article was originally published under the title "Beyond the Illusion: Disinformation and Deepfakes in the Age of AI" in NTT DATA's Cyber Frontiers magazine, January 2026 edition. It is reproduced with permission.

As AI blurs the line between what is real and what is fake, organizations must confront a new wave of digital deception that threatens trust, security, and the very notion of truth.

Human trust underpins many critical digital interactions with organizations and government entities. However, this trust is under threat, as AI enables the creation of deepfakes that impersonate real people through digital audio and video with remarkable accuracy. What once required specialized studios and considerable resources is now within reach of malicious actors with everyday computing resources and minimal technical knowledge.

What we are seeing is only the tip of the iceberg, as the scale of the problem is growing exponentially.

For government agencies, the national security implications are profound. The World Economic Forum Global Risks Report 2024 ranks AI driven misinformation and disinformation as the top threat the world will face over the next two years.

From a cybersecurity perspective, deepfakes represent a new threat vector. Traditional security frameworks, focused on system access and data protection, are not designed to identify content based deception. This creates a blind spot in security operations centers, leaving organizations vulnerable to a new generation of attacks that target human trust rather than technical systems.

The cybersecurity imperative

Deepfake detection is now a fundamental cybersecurity requirement. The convergence of AI enabled impersonation with traditional attack vectors creates compound threats that evade conventional security measures:

- Executives are being impersonated in video calls to authorize fraudulent transfers, creating significant financial risk.
- Voice cloning is increasingly used to defeat biometric authentication systems, compromising verification methods that were once considered secure.
- The use of synthetic media enables sophisticated phishing campaigns that are almost indistinguishable from legitimate communications.
- Manipulated evidence threatens to compromise legal and regulatory processes, undermining judicial integrity.
- Coordinated disinformation attacks against critical infrastructure raise national security concerns by eroding public trust and potentially disrupting essential services.

These threats require specialized detection capabilities integrated directly into security operations workflows. Without real time protection against synthetic media, even the most robust cybersecurity frameworks remain fundamentally incomplete.

Synthetic deception: Deepfakes targeting critical sectors

Deepfakes represent a powerful threat in high-risk sectors. In financial services, attackers use AI generated voice and video to impersonate banking customers during contact center calls, bypassing identity verification processes and initiating fraudulent transactions that exploit vulnerabilities in digital customer identity verification and voice-based authentication systems.

Government agencies are targeted through deepfake impersonation of officials and fabricated intelligence, posing risks to national security and public trust.

Critical infrastructure, including energy, healthcare, and emergency services, is vulnerable to disinformation campaigns driven by deepfakes that can simulate crisis communications, disrupt operational continuity, and confuse the public during emergencies. In the aviation sector, malicious actors could impersonate pilots, air traffic controllers, or airline executives using synthetic media, potentially causing flight delays and safety risks.

As these threats become more sophisticated, organizations need to invest in deepfake detection, secure communication protocols, and cross sector threat intelligence to safeguard trust and resilience.

Countering the deepfake threat: A multimodal defense strategy

To counter the way attackers now combine text, audio, images, and video to create convincing deception, defenses must be equally multifaceted.
Imagine the following scenario: a senior executive receives a late night call. The voice on the other end is unmistakable, it belongs to the CEO, urgently requesting a bank transfer. But it is a synthetic voice, cloned with unsettling accuracy. This is where audio forensics expertise comes into play. Advanced detection algorithms analyze subtle inconsistencies, unnatural pauses, frequency anomalies, and breathing patterns to expose the fake. Even when the voice sounds authentic, the system can recognize the difference.

Now imagine a video conference where a familiar face delivers instructions. However, behind the pixels lies a forgery. Deepfake video detection tools examine facial microexpressions, blinking patterns, and behavioral signals that reveal a synthetic origin. These tools act as digital lie detectors that protect visual communication channels from manipulation. But detection alone is not enough.

Real time response is also essential. Modern security systems integrate deepfake detection engines that operate continuously, flagging suspicious content the moment it appears.

Alerts are prioritized based on severity, ensuring that high risk threats are escalated without overwhelming security teams. Each incident is logged with detailed metadata, including timestamps, source data, and anomaly scores, creating a forensic trail that supports investigation and regulatory compliance.

In addition, these systems learn through built in auditing capabilities, analyzing patterns across incidents and helping organizations strengthen their defenses over time.

Whether preventing social engineering attacks or protecting the integrity of digital communications, the objective is clear: to restore trust in what we see and hear. In the battle against synthetic deception, a multimodal and intelligent defense is not optional, it is a necessity.

Preparing security operations for the future: Staying ahead of the synthetic curve

The deepfake threat evolves with every advance in AI capabilities. What seems innovative today may become commonplace tomorrow. In this shifting environment, organizations that act now lay the foundation for resilience against what lies ahead.

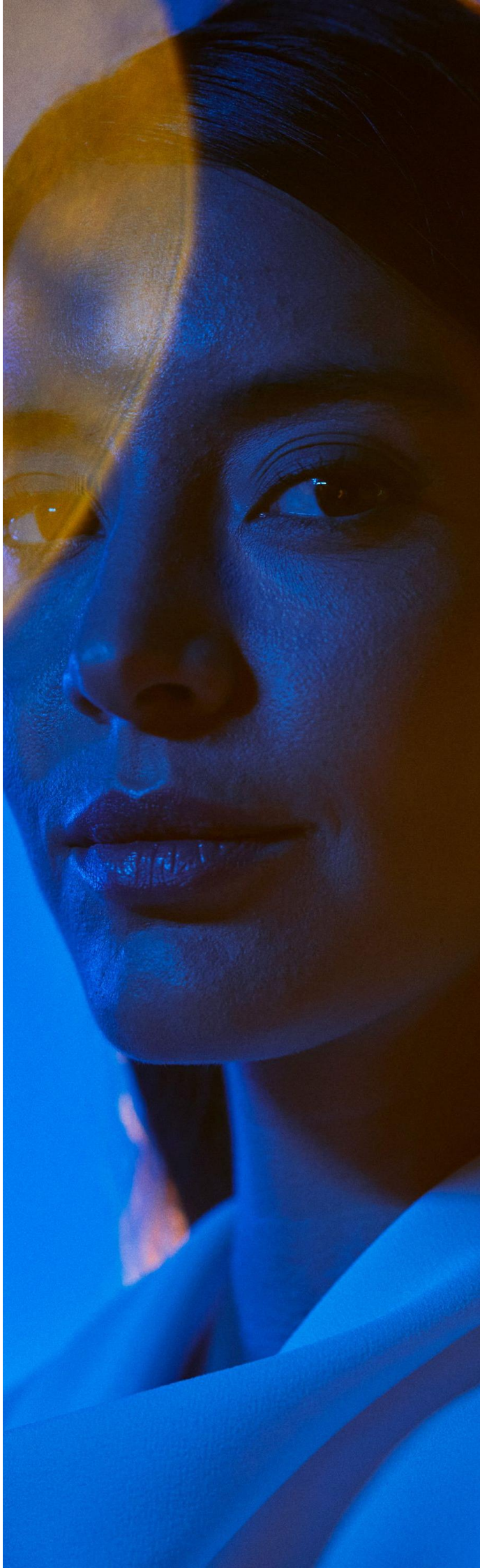
Deepfake detection should be understood as a strategic transformation. By integrating these tools into the core of security operations, organizations and governments are redefining how truth is verified in the digital age. It is no longer enough to trust what we see or hear, it must be verified through intelligence driven systems that adapt as quickly as the threats they are designed to counter.

This shift goes beyond technology; it is also about trust. Protecting communication channels from AI driven impersonation ensures that critical decisions are made based on authentic information. It preserves the integrity of leadership, the continuity of operations, and stakeholder trust.

In a world where synthetic media is increasingly convincing, defense against deepfakes becomes a fundamental pillar of digital trust.

Prakash Narayanamoorthy
Global Capability Leader: Emerging Technology Security at NTT DATA

Ben Colman
Co-Founder and CEO at Reality Defender



From Regulation to Practice: How Organizations Must Govern Artificial Intelligence

Article by Julissa Calderón Loayza and Melanie Brenis Valencia

The development and adoption of Artificial Intelligence (AI) are advancing at an increasingly rapid pace, generating clear benefits in efficiency, automation, and decision making, but also introducing new risks related to security, privacy, and transparency. As these systems are integrated into increasingly critical organizational processes, various states have intensified their efforts to establish regulatory frameworks that help manage these risks and provide greater legal certainty. In this context, it is relevant to examine the current state of AI regulation, offering below a general overview of its evolution across different countries in the Americas and Europe.

Europe: the first binding AI framework

In Europe, AI regulation took a decisive step forward with the approval of the **European Artificial Intelligence Regulation (EU AI Act)** in 2024, with progressive application starting in 2025. The regulation is directly applicable across the 27 Member States of the European Union and constitutes the first comprehensive and binding regional framework on AI. Its provisions apply to both public and private organizations that develop, market, or use AI systems in the European market, even if they are established outside the EU, provided that those systems have an impact within its territory.

At a general level, the EU AI Act establishes a regulatory model based on the risk level of the AI system and sets out, among others, the following key obligations:

- It prohibits certain AI uses considered unacceptable due to their impact on fundamental rights, for example, sensitive biometric categorization.
- It requires strict controls for high risk AI systems, including the implementation of a risk management system and human oversight.
- It imposes transparency obligations, especially when AI systems interact with individuals or generate synthetic content, for example, deepfakes.
- It defines clear responsibilities for providers, distributors, and users of AI, establishing oversight mechanisms by authorities.

The Americas: growing regulatory interest

In the Americas, unlike in Europe, AI regulation remains in an early stage. Most countries do not yet have specific laws in force, although a growing regulatory interest can be observed through legislative proposals in countries such as Chile, Brazil, Mexico, Colombia, Argentina, and Ecuador.

These initiatives seek to establish ethical principles, protect fundamental rights, and define basic transparency obligations, but most remain in early stages and lack clear oversight mechanisms, creating regulatory uncertainty.

Within this landscape, the most significant advances are concentrated in the United States and Peru. In the United States, although there is still no comprehensive federal AI law, several states have enacted regulations already in force, such as the **Colorado AI Act, the Utah AI Policy Act, and the Texas Responsible AI Governance Act**, which introduce concrete obligations regarding responsible use, transparency, and governance of AI systems. This approach, while fragmented, is operational and reflects regulatory progress at the state level.

Peru, for its part, has been one of the first countries in Latin America to develop a regulatory framework applied in an effective manner. It approved **Law No. 31814** in 2023, which promotes the use of AI for economic and social development, and subsequently issued **Supreme Decree No. 115-2025-PCM**, establishing clear provisions for its effective implementation.

Broadly speaking, the Peruvian framework, already in force, introduces obligations such as:

- Classification of AI systems according to their level of risk and purpose, requiring prior impact assessments and defining the degree of oversight applicable before deployment.
- Requirements for impact assessments and risk analysis for the use of AI in the public sector, considering effects on fundamental rights, security, and potential bias.
- Traceability and documentation requirements for AI systems, enabling their functioning, decisions, and outcomes to be explained to competent authorities.

- Explicit reference to international standards and best practices, such as ISO/IEC 42001, to guide the management, continuous monitoring, and improvement of AI systems.

The landscape described shows that AI regulation is advancing at different speeds, but with a common trend: the need to control the risks associated with its use. In this context, organizations cannot limit themselves to reacting to new regulations, they must understand their current position regarding AI usage. Having a clear assessment, identifying risks and gaps, and implementing appropriate measures are key to establishing an AI governance model that complements regulation and enables anticipation of future regulatory requirements.

AI Governance: from regulation to effective risk management

The regulatory progress described above confirms a reality: artificial intelligence is no longer just a technological issue, but a strategic, legal, and risk management matter. However, regulation alone does not guarantee responsible use. The real challenge for organizations is to translate these requirements into an internal governance model that enables risk control, ensures compliance, and sustains trust.

Today, a significant number of organizations already use AI in critical processes or are in advanced stages of adoption. Various international reports and studies agree that, although investment in AI continues to grow steadily, maturity in governance, risk management, and control remains limited. In many cases, initiatives emerge in a decentralized manner, with models or solutions implemented without a clear structure for oversight, traceability, or formal accountability. It is in this context that the need for AI governance arises.

What does governing AI involve?

Governing AI does not mean slowing down innovation but enabling it safely. It involves establishing a structured framework that supports the entire system lifecycle, from design and training to monitoring and eventual decommissioning, ensuring transparency, security, privacy, and regulatory compliance.

A solid AI governance model is typically built on five fundamental pillars:

1) Clear definition of roles and responsibilities:

It is essential to clearly define who is responsible for the data, the model, risk control, and security. Organizational ambiguity is one of the main sources of exposure. Without a clear allocation of responsibilities, risks become diluted and critical decisions lack proper oversight.

The governance structure will depend on the level of digital and organizational maturity. In companies with more advanced analytics and innovation capabilities, there may even be a Chief AI Officer (CAIO) with cross functional responsibility over strategy, risks, and AI oversight. In other cases, the role falls to the Chief Data Officer (CDO), when AI is closely tied to data governance, or to the CIO or CTO when the focus is more technological. Additionally, many organizations are establishing interdisciplinary AI committees that include leaders from technology, data, risk, compliance, legal, and cybersecurity, and even board members or senior management in cases of higher strategic exposure. This approach helps align innovation with risk appetite and executive oversight.

2) Risk management by design:

AI must be assessed using a risk based approach. This includes not only traditional technology risks, but also emerging risks such as algorithmic bias, lack of explainability, vulnerability to adversarial attacks, information leakage, reputational impact, and potential effects on fundamental rights. Risk management must be continuous, not a one time effort.

3) Integration with data governance and cybersecurity:

There is no trustworthy AI without governed data or robust security controls. The quality, legitimacy, and classification of data are critical. At the same time, AI expands the attack surface, requiring specific controls against threats such as model manipulation, data extraction, or misuse of generative tools by employees or third parties.

4) Corporate principles of responsible AI::

Beyond regulatory compliance, organizations must define their own principles for responsible use, such as transparency, human oversight, non discrimination, security, and accountability, and integrate them into their culture and decision making processes.

5) Integration with existing corporate governance:

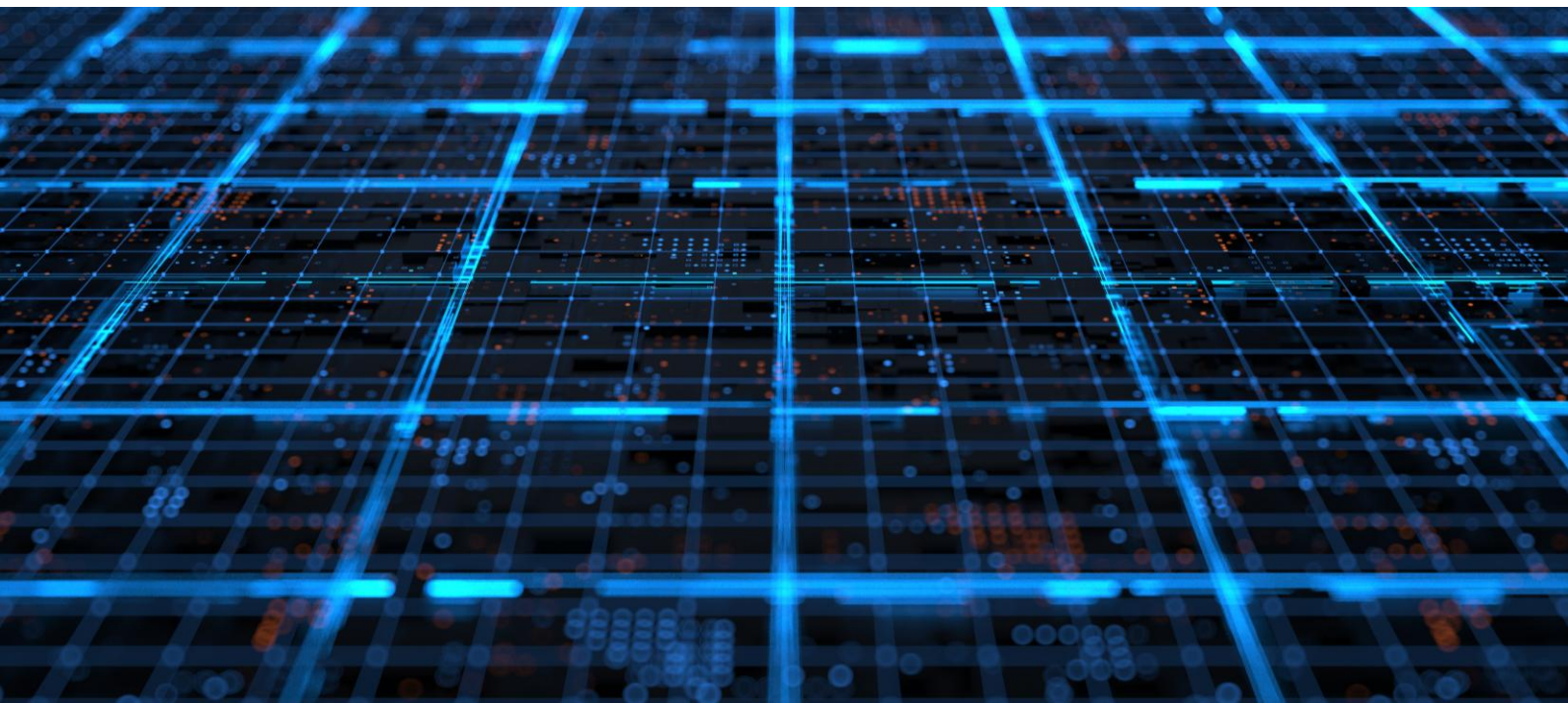
AI governance should not operate as a parallel structure, but be integrated with data governance, enterprise risk management, compliance, and cybersecurity. This integration avoids duplication and strengthens strategic coherence.

Trust as a competitive advantage

The evolution of AI cannot be limited to the technological dimension. Organizations that succeed in structuring a solid governance model will be better prepared to respond to regulators, mitigate incidents, and maintain the trust of customers and stakeholders.In an environment where regulation is advancing and reputational exposure is immediate, the competitive advantage will not lie solely in who innovates faster, but in who does so in a safer, more transparent, and responsible way. AI governance thus becomes the bridge between innovation and organizational resilience.

Julissa Calderón Loayza
Cybersecurity Expert Associate

Melanie Brenis Valencia
Cybersecurity Senior Consultant



Offensive Cybersecurity and Agentic AI Trends: Implications for the Modern Red Team

Trends by Marco Antonio Andazabal Rebaza

The evolution of Artificial Intelligence (AI) has transformed the interaction between users and technology, shifting from a tool for analytical support to systems capable of generating content, automating processes, and assisting in specialized technical tasks. This democratization has lowered the barrier to entry for advanced capabilities, allowing non specialist profiles to access functionalities that were previously reserved for experts. However, this accessibility also raises cybersecurity challenges. In the offensive domain, the emergence of agentic AI systems introduces a new paradigm: models capable of planning, executing, and adjusting actions autonomously to achieve defined objectives.

From Generative AI to Agentic AI

1) Generative AI and assisted automation

Generative AI, primarily based on large language models (LLMs), is characterized by its ability to produce content, including text, code, configurations, or technical analysis, in response to explicit instructions. Its operation is essentially reactive: it responds to a specific prompt without maintaining operational autonomy beyond the immediate interaction.

In the context of offensive cybersecurity, its application focuses on support tasks such as script generation, payload creation, drafting emails for phishing simulations, and similar activities.

However, these systems require constant supervision. Each step of the offensive process, including reconnaissance, exploitation, and post exploitation, must be manually directed by the operator. The AI does not make strategic decisions on its own, but instead executes tasks defined by human instructions.

2) Agentic AI: goal oriented systems with operational autonomy

Agentic AI represents a structural evolution compared to traditional generative models. Instead of being limited to responding to specific instructions, these systems are designed to achieve defined objectives through autonomous planning and execution processes.

From a theoretical perspective, an agentic system integrates:

- Multi step planning, breaking down a complex objective into sub tasks.
- Persistent contextual memory, maintaining state and action history.
- Autonomous execution: it interacts with external tools such as APIs, operating systems, and scanners.
- Evaluation and feedback: it analyzes results and adjusts its strategy.

Architecturally, it combines a language model with an iterative decision cycle, perception, planning, action, and evaluation. This allows it to operate as an “agent” within a technical environment, rather than as a passive assistant.

Transformation of the Red Team in the age of Agentic AI

1) Advanced automation of reconnaissance

In Red Team operations, the reconnaissance phase is critical. It typically involves manual or semi automated information gathering using OSINT tools, network scanners, and analysis of exposed attack surfaces.

An agentic AI system could:

- Define sub objectives, such as identifying domains, subdomains, and exposed services.
- Orchestrate multiple scanning tools.
- Correlate results.
- Prioritize attack vectors based on likelihood of success.
- Adjust its strategy based on intermediate findings.

This behavior more closely resembles that of a human operator supported by intelligent automation than that of a simple static script.

Dynamic exploit generation and proof of concept development

While generating complex exploits still requires specialized knowledge, AI can assist in:

- Adapting public exploits to specific contexts.
- Modifying payloads based on environmental constraints.
- Generating scripts for proof-of-concept testing.
- Conducting preliminary analysis of vulnerable code.

In a controlled pentesting scenario, this can significantly reduce the time between identifying a vulnerability and validating it technically.

However, the concern lies in the fact that malicious actors could use similar capabilities to scale attacks with less technical expertise

AI assisted social engineering

One of the most significant impacts is observed in social engineering. Agentic AI can:

- Analyze public profiles.
- Generate highly personalized emails.
- Adjust tone based on organizational role.
- Simulate coherent conversations across multiple iterations.

This increases the potential success rate of targeted phishing campaigns, spear phishing, while reducing the need for advanced psychological manipulation skills.

The convergence of offensive cybersecurity and agentic AI is redefining the traditional dynamics of Red Team operations and technical pentesting. The transition from reactive models to autonomous, goal oriented agents introduces a structural shift in how offensive operations are executed and scaled.

More than just an automation tool, agentic AI represents a strategic catalyst capable of amplifying both defensive efficiency and offensive potential. In this context, the challenge lies not only in understanding the technology, but in anticipating its operational, ethical, and regulatory implications.

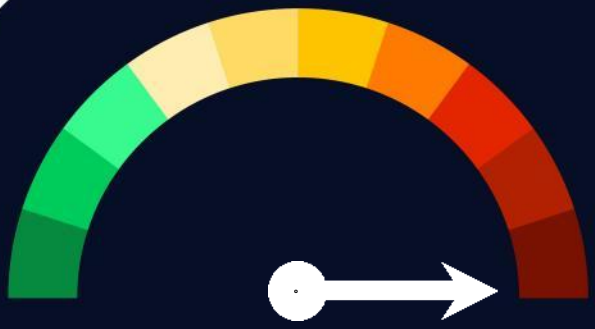
The future of cybersecurity will not depend solely on technical capability, but on the intelligent governance of increasingly autonomous systems.

Marco Antonio Andazabal Rebaza
Cybersecurity Analyst

Vulnerabilities

Vulnerabilities in Cisco Secure Firewall Management Center

Date: March 4, 2026
CVE: CVE-2026-20079 and CVE-2026-20131



CVSS: 10.0

CRITICAL

Description

Two critical vulnerabilities have been identified, classified as CVE-2026-20079 and CVE-2026-20131, affecting Cisco Secure Firewall Management Center.

The first vulnerability, CVE-2026-20079, is due to an incorrect process created during system startup. An attacker could exploit this flaw by sending a malicious HTTP request. This could allow the attacker to execute scripts and commands on the affected system and obtain root privileges.

The second vulnerability, CVE-2026-20131, involves the insecure deserialization of a user provided Java byte stream. An attacker could send a serialized Java object to execute code on the device and gain root privileges.

Solution

The vendor recommends updating affected products to the latest version.

To do so, Cisco advises its customers to use the Cisco Software Checker and follow its instructions.

Affected Products

The affected products are as follows:

- Cisco Secure FMC Software
- Cisco Security Cloud Control (SCC) Firewall Management

References

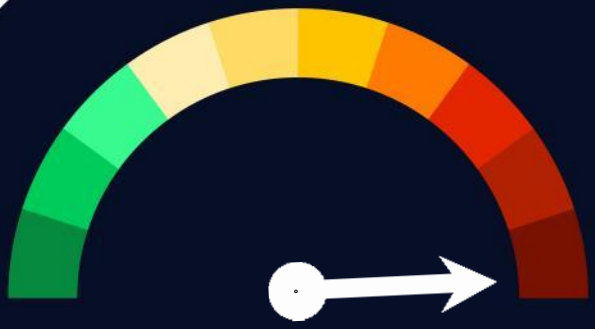
- sec.cloudapps.cisco.com
- sec.cloudapps.cisco.com
- incibe.es

TLP:WHITE

Vulnerabilities

Critical Vulnerability in Android (System)

Date: March 2, 2026
CVE: CVE-2026-0006



CVSS: 9.8

CRITICAL

Description

A critical remote code execution vulnerability has been identified in Android devices across multiple versions.

This vulnerability, CVE-2026-0006, allows an attacker to execute malicious code without requiring user interaction or additional privileges, as it resides in a core Android System component.

Successful exploitation could enable full remote control, data exfiltration, real time surveillance, installation of persistent malware, and lateral movement.

Solution

It is recommended to install the update corresponding to the March 1, 2026 security patch level or later.

Manufacturers such as Google, Samsung, and Xiaomi are deploying these updates via OTA (over the air).

Affected Products

Devices running Android versions 12, 12L, 13, 14, and 15 are affected by this vulnerability.

References

- source.android.com
- nvd.nist.gov

TLP:WHITE

Android fixes 129 vulnerabilities in its March security patch

Date: March 2, 2026
CVE: CVE-2026-21385 y 128 más

Critical

Description

The August Android Security Bulletin addresses a total of 129 vulnerabilities, including 10 classified as critical and 106 as high severity. Exploitation of these vulnerabilities could allow an attacker to achieve privilege escalation, remote code execution, or trigger a buffer overflow.

Android indicates that the vulnerability identified as CVE-2026-21385 may be under limited exploitation. This vulnerability is located in a Qualcomm display component. The company stated that the flaw resides in the Graphics subcomponent and consists of an integer overflow that an attacker could exploit to cause memory corruption on the device.

Affected Products

The products affected by this vulnerability include:

- Android versions prior to March 1, 2026.

Solution

Update affected products to the latest available version.

References

- source.android.com
- docs.qualcomm.com

Google releases urgent fixes for 10 vulnerabilities

Date: March 3, 2026
CVE: CVE-2026-3536 and 9 more

High

Description

Google has released an urgent security patch for Chrome to address 10 vulnerabilities, including 3 classified as critical and 7 as high severity.

Among the identified issues are memory corruption vulnerabilities and implementation flaws in graphics and JavaScript engines, which could allow arbitrary code execution, data exfiltration, among other impacts.

The most critical vulnerabilities, CVE-2026-3536, CVE-2026-3537, and CVE-2026-3538, are related to validation gaps in web and browsing codecs, which could hinder the detection of phishing and unauthorized downloads.

Users and organizations are advised to apply the updates as soon as possible.

Affected Products

The products affected by this vulnerability include all versions of Google Chrome prior to:

- Version 145.0.7632.159.

Solution

It is recommended to update to the latest software versions.

References

- cyberpress.org
- nvd.nist.gov

Events

IAPP Global Summit 2026
March 30 to April 2

The IAPP Global Privacy Summit 2026 will take place from March 30 to April 2, 2026, in Washington, D.C., as an in person event, establishing itself as one of the key global gatherings in privacy and cybersecurity. The event will bring together leaders from the public and private sectors to discuss international regulation, data governance, emerging cyber risks, and the real impact of artificial intelligence on information protection. It is a strategic forum for anticipating trends and regulatory challenges.

Link

Gen AI Summit
April 17 to 18

The Gen AI Summit EU 2026 will take place from April 17 to 18, 2026, in Valencia, Spain, as a two day in person event designed for AI, data, and machine learning professionals. The event will bring together technology leaders, innovators, and technical teams to explore the transformative potential of generative artificial intelligence. The agenda includes technical talks, panels on ethics, governance, and security, as well as networking opportunities and hands on workshops.

Link

CYBERUK 2026
April 21 to 23

CYBERUK 2026 will take place from April 21 to 23, 2026, at the Scottish Event Campus (SEC) in Glasgow, United Kingdom, as an in person event. Organized by the National Cyber Security Centre (NCSC), it is the UK government's flagship conference for cybersecurity professionals, featuring more than 100 expert speakers. The program addresses the theme "The Next Decade: Accelerating Our Cyber Defence," exploring strategies, emerging threats, critical defense, and public private collaboration. It will also include exhibition areas, networking opportunities, and specialized technical sessions.

Link

Cyber Intelligence Europe 2026
April 22 to 23

Cyber Intelligence Europe 2026 will take place from April 22 to 23, 2026, in Brussels, Belgium, as a two day in person event. Organized with a focus on European cooperation, it will bring together representatives from governments, armed forces, and security agencies to discuss national cybersecurity strategies and public policy. The program includes analysis of cybercrime trends, threat monitoring, and preparedness for cyberattacks, with particular attention to the protection of critical infrastructure. The event will also explore coordinated approaches to data sharing and joint responses to large scale threats.

Link

Resources

- **Integrating Cybersecurity and Enterprise Risk Management (ERM) - NIST**

An NIST publication that provides guidance to organizations on integrating cybersecurity into the Enterprise Risk Management (ERM) framework, aligning the identification, assessment, and prioritization of cyber risks with business strategic objectives. The document explains how to use risk registers to improve executive level decision making and strengthen communication between technical teams and senior management, promoting stronger governance and greater resilience against digital threats.

Link

- **The ENISA Cybersecurity Exercise Methodology - ENISA**

An ENISA publication that provides a comprehensive theoretical framework for planning, executing, and evaluating effective cybersecurity exercises from start to finish, ensuring that the appropriate profiles and stakeholders are involved at the right time. It is based on lessons learned, industry best practices, and cybersecurity expertise, along with practical tools and templates to organize and enhance simulations and incident response testing.

Link

- **Compendium on Personal Data Protection: Relevant Regulations and Interpretative Criteria**

An official document published by the Ministry of Justice and Human Rights of Peru that compiles, in an updated manner, the Personal Data Protection Law No. 29733, its regulation, and relevant interpretative criteria issued by the National Authority for Personal Data Protection to guide the practical application of the regulatory framework. It serves as a reference for public and private entities in managing and ensuring compliance with personal data protection laws.

Link

NTT DATA

Suscribe to RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com