Issue 111 | February 2026

NTT DATA

Radar

The Cybersecurity Magazine

Cybersecurity starts, and ends, with people

By Francisco Javier García Lorente

For years, cybersecurity has been treated as a predominantly technological problem. More robust firewalls, more sophisticated detection tools, or artificial intelligence applied to threat monitoring. All of that is necessary. All of that is valuable. However, it is not sufficient. The reality, supported by data and experience, is unequivocal: the majority of security incidents still originate with people. Not through ill will, but owing to a lack of awareness, overconfidence, or simply ingrained poor habits.

This is where a key concept comes into play, one that many organizations still underestimate: cybersecurity culture. And, more specifically, the role of human leadership as the driving force behind that culture.

Speaking about cyber culture is not about policies posted on an intranet site, nor about mandatory training sessions that are forgotten as soon as the browser window is closed. Speaking about culture means referring to repeated behaviors, everyday decisions, and attitudes towards risk. And culture, whether we like it or not, is shaped from the top..

Leadership through example: actions carry more weight than words

Organizations do not change because a message is sent to their inbox. They change when leaders act in a consistent and visible manner. In cybersecurity, this is particularly critical. A senior manager who shares passwords "for convenience", bypasses multi-factor authentication "because it's inconvenient" or downplays an incident with "nothing really happened", is sending a clear message to the organization: security is secondary.

By contrast, leadership that integrates cybersecurity into its decision-making, that asks questions, shows curiosity, respects established processes, and speaks openly about risks and lessons learned, creates a multiplier effect. Leaders do not need to be technical experts. They need to be aware of the influence they hold.

Culture cannot be enforced. It is adopted.

One of the most common mistakes in cybersecurity programmes is treating employees as the "weakest link". This narrative, besides being unfair, is counterproductive. People are not the problem; they are the solution, provided they receive the right context, tools, and support.

And once again, leadership is decisive. Leadership that cultivates a culture of fear—fear of mistakes, of repercussions, of "getting it wrong"—creates silence. And silence, in cybersecurity, is fatal. Incidents go unreported, suspicious emails are ignored, and mistakes are concealed until it is already too late.

Human-centered leadership, by contrast, normalizes error as part of the learning process, encourages early reporting, and recognizes good practice. It turns employees into active risk sensors rather than passive recipients of rules.

Cybersecurity as a value, not a barrier

Another major cultural challenge is the perception of cybersecurity as an obstacle to the business. "This slows things down", "this complicates everything", "this isn't practical". When that message takes hold, security is experienced as an external imposition.

Leadership has the responsibility to reframe the narrative: cybersecurity does not hinder the business; it protects it and enables its sustainability. It is not a cost; it is an investment in trust, reputation, and continuity. In an environment where clients, partners, and regulators increasingly demand assurance, security is no longer optional. When leaders embed this perspective into their strategic narrative, the organization begins to understand that working securely is simply working properly.

Human leadership in a complex digital environment

We operate in a context of hyper-connectivity, hybrid work, digital supply chains, and increasingly sophisticated threats. Believing that this environment can be controlled through technology alone is a dangerous illusion. The human factor is unavoidable, and precisely for that reason, it must be managed intelligently.

Human leadership in cybersecurity requires empathy, clear communication, and consistency. It involves tailoring messages to different audiences, understanding real day-to-day pressures, and designing security measures that support users rather than placing them at odds with the system. Technology protects, and leadership aligns.

Continuous learning, not one-off events

A strong culture is not built through isolated campaigns. It is built through consistency. And once again, leadership makes the difference: when cybersecurity training is perceived as strategic, recurrent, and aligned with the realities of the business, it stops being an obligation and becomes a valuable tool.

Leaders must promote training that is dynamic, practical, and contextualized—training that evolves alongside emerging threats and the organization itself. It is not about knowing everything; it is about knowing how to respond.

Conclusion: to lead is to protect

Ultimately, discussing cybersecurity culture and leadership is a discussion about responsibility. Cybersecurity is not only a matter of systems; it is a matter of people, decisions, and values. And values must be led.

Organizations that understand this do not look for someone to blame after an incident; they look for lessons learned. They do not place blind trust in technology; they trust their teams. They do not delegate security solely to a single department; they integrate it into their organizational DNA. Because in today's digital world, to lead is also to protect. And protection begins with people.

Francisco J. Garcia Lorente
Cybersecurity Project Manager

Shai-Hulud 2.0: the day the worm understood the full chain

Cyber-chronicle By Leire Cubo Arce

We close the year with December once again proving to be one of the most active months in the cybersecurity landscape. While organizations slow down due to holidays and reduced staffing, cybercriminals take full advantage of the season, intensifying campaigns that exploit both technical vulnerabilities and human trust.

One of the most significant events of the month has been the disclosure of a critical vulnerability affecting MongoDB, identified as CVE-2025-14847 and commonly referred to as MongoBleed. This flaw allows attackers to extract sensitive information from affected databases without authentication, posing a severe risk to organizations relying on exposed or improperly configured MongoDB instances. Security researchers have confirmed active exploitation attempts shortly after disclosure, reinforcing the importance of rapid patching and strict access controls on data infrastructure.

December has also been marked by Microsoft's end-of-year Patch Tuesday, which addressed more than fifty vulnerabilities across its ecosystem. Particularly concerning were several zero-day flaws that were already being exploited in the wild, enabling remote code execution and privilege escalation. These vulnerabilities once again highlight how widely used enterprise platforms remain a prime target for attackers seeking scalable impact.

Beyond traditional IT environments, operational technology has continued to draw attention. Throughout this month, CISA released multiple security advisories affecting industrial control systems and medical devices from well-known manufacturers. These advisories underline the growing convergence between IT and OT and the increasing exposure of critical infrastructure to cyber threats, especially in sectors where patching cycles are slow or operational downtime is difficult to accept.

Ransomware activity has shown no signs of slowing as 2025 comes to an end. Threat actors have continued to target healthcare organizations, public administrations and service providers, often leveraging previously stolen credentials or vulnerabilities in third-party software. Analysts have observed that many of these attacks rely on long-standing initial access, reinforcing the idea that attackers are patient and opportunistic, waiting for the right moment to strike.

At the same time, threat reports published during December have revealed the scale of credential exposure circulating on underground forums, with billions of compromised usernames and passwords available to cybercriminals. This massive availability of credentials fuels automated attacks such as credential stuffing and account takeover, making identity protection and multi-factor authentication more critical than ever.

Geopolitical tensions have also been reflected in cyberspace. Reports released at the end of the year indicate sustained and large-scale cyber activity targeting critical infrastructure in the Asia-Pacific region, particularly against financial institutions, hospitals and government entities. These campaigns are widely associated with cyber-espionage and hybrid warfare strategies, demonstrating how cybersecurity is increasingly intertwined with global stability.

Data breaches have continued to impact citizens directly. The disclosure of a breach affecting a major healthcare portal in New Zealand revealed the exposure of hundreds of thousands of sensitive medical documents. The incident has reignited discussions around data protection, regulatory oversight and the responsibilities of digital health service providers.

Finally, this has also been a month of reflection for the cybersecurity community. Several analyses published towards the end of 2025 have questioned whether traditional security frameworks are adequately prepared for emerging threats linked to artificial intelligence. Issues such as prompt injection, model poisoning and AI-driven automation are pushing organizations to rethink how security controls are designed and applied in an increasingly AI-enabled world.

As 2025 comes to a close, December leaves a clear message: cyber threats continue to evolve across technical, human and geopolitical dimensions. Entering the new year, vigilance, timely patching, and adaptive security strategies remain essential to counter an ever-changing threat landscape.

Leire Cubo Arce
Cybersecurity Consultant

Leadership and Digital Transformation: from controlling employees to empowering human *firewalls*

Article by Isabel Lopez and David Contel

During its early stages—and for many years thereafter—digital transformation was understood largely as a matter of technological implementation. The main actors were tools, software, security, and control, to name just a few. However, for digital transformation to be truly effective—and cybersecurity is no exception—it does not begin with systems, but with the people who carry it out and the way in which they are led.Throughout history, organisations have developed a variety of leadership models that reflected not only personal styles but also social ones, which in turn mirrored political forms of governance and a certain collective unconscious within society.

Classical leadership versus modern leadership

The first is what we might define as classical leadership. Historically, it has been effective within organizations, operating under the assumption of a corporate culture in which employees needed to be supervised in order to meet their objectives. Its underlying premise was one of implicit mistrust, direct oversight, and the perceived risk of employees neglecting their responsibilities or procrastinating.

Translating this paradigm into the field of security would lead to measures such as limiting access, blocking websites, monitoring employees through a SIEM, and, ultimately, shielding the organization. Security would be understood as an expense, a purely technical issue, and even a disciplinary one.

In practice, however, the outcomes of digital transformation would be significantly limited. Even if systems were properly secured, the true agents of transformation, the daily users, would not develop a sense of responsibility for their cybersecurity practices. In other words, they would not believe that they themselves are an essential part of the solution to preventing security incidents and, in turn, contributing to the transformation of corporate culture, an element that is vital for digital transformation to be effective.

On the opposite end of the spectrum lies modern leadership. With all the nuances that such a shift implies, one of its foundational ideas is that people can, and should, be active agents of change. This paradigm inevitably requires that, in order for employees to become genuine protagonists, they must be empowered.

The specific competencies to be acquired will be defined by each organization in line with its corporate culture and, more pragmatically, through its internal policies. Regardless of each organization's particular identity, we can begin with the classic distinction between *hard* and *soft skills.*

On one hand, organizational users must be trained in good information-security practices, security policies, or more technical or ad hoc competencies depending on their role.

However, even more important than knowledge itself are personal competencies, and there is one in particular that the organization must foster across all its layers: empowerment. It is essential that employees not only know how to respond to a potential fraud attempt or security incident but also believe that they can do so; that they can support their colleagues; and, even more importantly, that they can make proposals—grounded in their operational expertise—to strengthen the organization's security. In short, each employee must internalize that they are part of the solution.

When this approach is put into practice, it leads to a positive scenario in which technical security is complemented, and, to some extent, can even compensate for certain security vulnerabilities, thanks to the human firewall created by empowered users.

What drives change?

Even when transformations are implemented within organizations, not all leaders promote change for the same reasons. In cybersecurity, the factors that typically drive meaningful change include regulatory requirements, incidents affecting the organization itself or direct competitors, and strategic intent.

Over recent years, **regulatory bodies** have emerged that require organizations to establish information-security management systems (LPIC, NISD, or various ISO standards). These regulations oblige companies to implement changes that, from an executive-level perspective, may be perceived as an expense. In any case, this external trigger has been a driver of transformation, albeit one with many nuances.

There is a popular Spanish expression that applies well to cybersecurity scenarios: *"cuando veas las barbas de tu vecino cortar, pon las tuyas a remojar"*. The dynamics of the free market naturally lead companies to monitor what their immediate competitors are doing.

This observation extends not only to products, commercial strategies, or market synergies; **direct competitors** often act as a mirror reflecting the threats that any organization might eventually face. A cyberattack is a very real possibility, not only because of operational consequences, but also due to potential regulatory sanctions. In practice, this becomes a strong motivator for change, again, with its own nuances.

However, the true driver of genuine transformation is strategic choice. In other words, when executives and organizational leaders view information-security management not merely as an investment, but as an opportunity to differentiate themselves, protect the organization, and set an example as a brand in the market. This internal driver is what can truly disseminate change across all layers of the organization, since leadership commitment is essential for the effectiveness of any initiative.

The role of the leader in digital transformation

Middle managers are an essential element in any digital transformation, as they are the ones who actually deploy changes in day-to-day operations.

The same leadership principles outlined earlier apply equally to this tier of the hierarchy.

Not only do middle managers influence the fulfilment of operational objectives, but also the way in which those objectives are achieved. Classical leadership creates dependence on the manager's instructions. However, a more modern perspective, one in which not only competencies but also decision-making authority and initiative are delegated to team members, enables more effective implementation, as users themselves become responsible for delivering change. Moreover, middle managers act as a powerful amplifier for organizational policies or new initiatives, often more effective than a communications department.

Conclusion

Leadership has evolved over time to adapt to the shifting realities of the world. However, the way it is exercised depends on cultural variables, personal traits, and professional experience.

All of this suggests that the way organizations and teams operate today will inevitably evolve in the future. Yet, regardless of the specific leadership style, one thing remains indisputable: the involvement of all users within an organization in any transformation process leads to significantly better outcomes.

Isabel Lopez
Cybersecurity Consultant

David Contel
Cybersecurity Expert Consultant

The path upward and the path downward are one and the same: cybersecurity, seamanship, and leadership.

Article by Jorge Ortí Navarro

Víctor López Barrantes, Country Manager of NTT DATA Spain, shared in corporate communications in April 2025 that inspiring leadership is essential for our future. In the same vein, Abhijit Dubei, President and CEO of NTT DATA, Inc., expressed that leadership is not limited to titles or positions; rather, we must actively commit and take responsibility for the future we are building. He emphasised the importance of being ready each day to inspire, empower, and care—and he encourages all of us to be leaders, whatever our role may be.

In a world like cybersecurity, where new threats emerge daily and where certainties are scarce, organizations need, more than ever, leaders capable of offering direction and balance without hindering progress.

And since the cyber world is one of questions and uncertainty, it is worth asking: how can we establish a leadership model that is able to foster a security culture that is conscious, stable, and, above all, able to advance in an environment of constantly evolving threats?

The classics have already taught us that the path upward and the path downward are one and the same. Taking this lesson as our guiding principle, we found the answer in a place where one might least expect it: in the art of navigation.

Let us start at the beginning: ships. The Royal Spanish Academy defines a vela (“sail”) as the piece of canvas or other material that is fixed to spars in order to catch the wind and propel a vessel. Secondly, it defines the ancla (“anchor”) as an iron instrument formed by a bar with curved hooks, attached to a chain and dropped to the seabed to secure the vessel. Finally, the orza (“centreboard” or “keel fin”) is the piece that increases the draft of a boat, providing greater stability and improved steering when sailing close to the wind.

In this context, Jesús Terrés published the article Ser orza y no ancla on 5 March 2022, in which he distinguishes three types of people. First, the “sail person”: someone who never hesitates, who is driven by impulse, who fears neither adventure nor braking too late nor derailing altogether. They do not mind starting the evening in Valencia and ending it at Berghain, Berlin’s legendary nightclub.

A “sail” decides purely by emotion, without a trace of rationality. Passionate and drawn to the unexpected, this person will never prevent drifting, because drifting is part of their very nature.

Letting oneself drift, ultimately, driven by impulse and unable to brake in time, ends with the vessel stranded in unfortunate ports.

The “anchor person”, by contrast, is someone who prevents progress. As Jesús explains in his article, when we speak of people who are anchors, we refer to them as a burden, someone or something immobile that neither moves nor allows you to move forward. They fasten themselves to a rock, to a sandy seabed that keeps the boat from advancing. It may even be that, if the anchor is dropped while a fierce wind is blowing, its resistance could end up breaking the boat itself, precisely because the anchor holds it rigidly in place.
The “centreboard person”, however, is quite the opposite. They do not brake, like the anchor. They do not prevent you from reaching Berlin. The centreboard simply provides stability, and not in a negative sense. Stability is what enables progress, what keeps things from coming to a halt, and at the same time prevents harm when the storm hits.

Perhaps this is what the sea and sailing have to teach us: that stability may be the greatest quality a person, and, by extension, a leader, can possess. These are the people we turn to in order to share the good and confide the bad, because it is in their steadiness that we find calm, or perhaps something all of us seek at some point: a guide.

A reference point that allows us to sail at full speed across the seven seas, against wind and tide, without capsizing. Without drowning in the chaos we sometimes encounter in the world of cybersecurity.

The “centreboard” will never prevent growth, progress, transformation, or evolution. They will support those who need it, care about their needs, and, above all, ensure that through those changes, those adventures, those seemingly impossible projects, we do not end up stranded on a deserted island or at the bottom of the sea. Instead, even in the fiercest storm, with gales or towering waves, we will always reach a safe harbour.

This is the kind of leader Abhijit Dubei refers to: someone capable of providing the stability needed to think, reflect, and keep fighting. The “centreboard” is not a “sail”, but it allows us to move fast without capsizing. It is a piece few people know, one that can easily go unnoticed and yet, without it, a sailing boat would always be either drifting or anchored. Support, constant steadiness, joy in the successes of others. The sensible impulse that enables us to continue working each day.

In the words of the aforementioned Jesús Terrés:

To be a centreboard and not an anchor; to try to make better the people you love (and never hold them back), to be nourishment and not a ceiling, a path and not mud. To withstand (together) the tides, to make things easy, to let others be, windows wide open, to know yourself sheltered but never confined, that my world may be your net, that you may allow yourself to fall: that will be my triumph [...]. To be your centreboard and not your anchor.

The path upward and the path downward are one and the same. Perhaps seamanship and cybersecurity are, too. Perhaps both require the same leaders. The same stability. Let us therefore be the centreboards that sustain the environment in which we work each day, an environment we can all feel proud to be part of.

Jorge Ortí Navarro
Cybersecurity Expert Consultant

Key Cybersecurity Trends in 2026

Trends by Diego Turiegano de las Heras

In 2026, cybersecurity will be shaped by a very clear shift in the way digital attacks are carried out and defended against. The advancement of generative artificial intelligence, the increasingly realistic use of deepfakes, and the automation of cybercrime will make the landscape more complex and harder to control. Threats will no longer rely as heavily on advanced technical expertise, but rather on increasingly accessible tools that enable sophisticated attacks to be launched with minimal effort. This will force companies and users alike to rethink how they protect themselves in an environment where the digital realm is now embedded in almost every daily activity.

Artificial intelligence will play a key and somewhat contradictory role. On the one hand, it will help strengthen cybersecurity by enabling faster threat detection, the analysis of large volumes of data, and more informed decision-making for security teams.

On the other hand, it will become a powerful tool for attackers, who will use it to automate tasks, craft more convincing messages, and tailor attacks to each individual target. This dual use of AI will continue to narrow the gap between attack and defence, raising the overall level of risk.

One of the most concerning developments will be the use of deepfakes as a fraud mechanism. By 2026, these fabricated contents will no longer be occasional occurrences; they will be used routinely to impersonate individuals and deceive both people and organizations.

Voice forgeries, in particular, will become increasingly realistic and easier to produce, enabling highly targeted scams such as fraudulent phone calls pretending to be senior executives or colleagues. Moreover, the lack of reliable systems for identifying AI-generated content will make detecting such deceptions even more challenging.

Real-time deepfakes will also begin gaining prominence; capable of altering a person's image or voice during a video call. Although they currently require a certain degree of technical sophistication, their rapid evolution will allow them to be used in more direct attacks, especially in professional environments where a high level of trust is placed in visual and voice communication.

This will cast doubt on traditional verification methods that rely simply on "recognizing" the person on the other side of the screen.

The automation of cybercrime will be another major shift.

In 2026, artificial intelligence will be used across every phase of an attack; from malware creation to vulnerability scanning and the distribution of malicious software.

This will enable faster, larger-scale attacks, reducing the amount of time security teams have to react.

In addition, the use of open-source AI models, which typically have fewer control mechanisms, will make it easier for these technologies to be used for both legitimate and criminal purposes, complicating attack analysis and attribution.

Despite all these technological advances, the human factor will remain one of the main weaknesses.

Credential theft will continue to be one of the most effective ways to gain access to systems, largely because many people still use weak passwords, reuse them across multiple services, or bypass multi-factor authentication.

Attackers will exploit this scenario through increasingly sophisticated social-engineering techniques designed to deceive users and trick them into carrying out actions that appear legitimate.

Ransomware will not disappear either. On the contrary, by 2026 it will be more widespread and faster. "Attack-as-a-service" models will allow individuals with limited technical skills to launch complex attacks using ready-made tools.

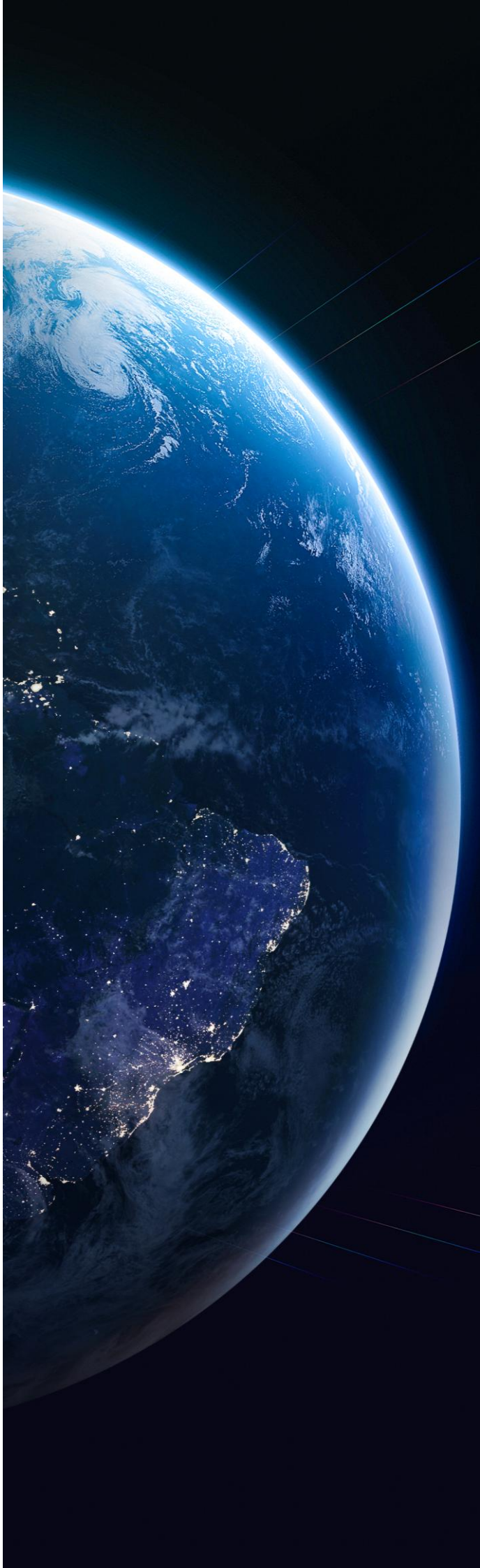
Artificial intelligence will help automate processes such as data encryption, information exfiltration, or even ransom negotiation, reducing victims' response time and increasing the impact of attacks.

Finally, the widespread adoption of artificial intelligence within companies will introduce new risks linked to the digital supply chain.

Many solutions will be deployed without sufficient security analysis, incorporating dependencies and potential vulnerabilities. At the same time, the malicious use of AI will continue to grow, with increasingly personalized phishing campaigns, more effective fraud bots, and the first cases of *malware* developed with the help of these technologies.

In this context, the major challenge in 2026 will be finding a balance between harnessing the benefits of artificial intelligence and controlling the risks it introduces, by prioritizing prevention, training, and a more conscious approach to risk management.

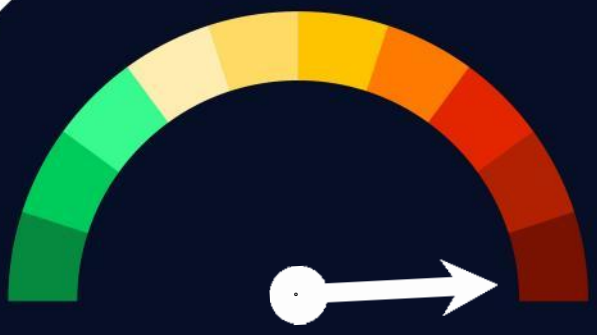
Diego Turiegano de las Heras
Cybersecurity Consultant



Vulnerabilites

Critical Vulnerability in n8n

Date: 26 December 2025
CVE: CVE-2025-68668



CVSS: 9.9

CRITICAL

Description

A critical vulnerability, **CVE-2025-68668**, has been identified in n8n, an open-source workflow automation platform.

This vulnerability allows authenticated users to execute arbitrary commands on the underlying system. The flaw is caused by an issue within the protection mechanisms of the Python Code Node, which makes it possible to escape the isolated environment and run code with the same privileges as the n8n process.

Although exploitation requires authentication and permissions to create or modify workflows, it is considered a high-risk issue due to the possibility of executing commands directly on the host.

Solution

It is strongly recommended to update immediately to the officially patched versions of n8n:

Version 2.0.0 or later

As a temporary mitigation, the following measures are advised:

- Disable the *Code Node* using the environment variable: NODES_EXCLUDE: "[\"n8n-nodes-base.code\"]“.
- Disable Python support in the node with: N8N_PYTHON_ENABLED=false.

Affected Products

The vulnerable versions are:

- From version 1.0.0 up to (but not including) version 2.0.0.

References

- nvd.nist.gov
- thehackernews.com

TLP:WHITE

Vulnerabilities

Critical vulnerabilites in *routers* D-Link DSL

Date: 5 January 2026
CVE: CVE-2026-0625

CVSS: 9.3

CRITICAL

Description

A critical remote-code-execution vulnerability **(CVE-2026-0625)** has been identified affecting several older, end-of-support D-Link DSL routers.

The flaw is caused by a command-injection issue in the DNS configuration *endpoint* (dnscfg.cgi), which allows a remote, unauthenticated attacker to execute commands with system-level privileges.

This vulnerability is currently being actively exploited and may lead to complete router compromise, DNS hijacking, traffic interception, or integration into botnets.

Solution

No official patch exists for most of the affected models.

It is recommended to:

- Replace the vulnerable devices.
- Disable remote administration.
- Restrict access through firewall rules / ACLs..

Affected Products

Routers D-Link DSL (EoL models), including:

- DSL-2640B
- DSL-2740R
- DSL-2780B
- DSL-526B

References

- incibe.es
- thehackernews.com

TLP:WHITE

IBM Fixes a Critical Authentication Bypass Vulnerability

Date: 31 December 2025
CVE: CVE-2025-13915

Critical

Description

IBM has released security updates for API Connect to address the critical authentication bypass vulnerability identified as **CVE-2025-13915**, which carries a CVSS score of 9.8.

This security flaw could allow a remote attacker to access protected services without valid credentials, compromising the confidentiality and integrity of the APIs managed by the platform.

IBM has indicated that the vulnerability can be exploited remotely and without user interaction, which significantly increases the risk for enterprise environments exposed to the internet. For this reason, it is strongly recommended to apply the security updates as soon as possible.

Affected Products

Vulnerable versions of IBM API Connect are:

- Versions from 10.0.8.0 to 10.0.8.5.
- Version 10.0.11.0.

Solution

It is recommended to:

- Immediately apply the patches and fixes provided by IBM (download and install the update available for API Connect from Fix Central according to the affected version).

References

- thehackernews.com
- incibe.es

OWASP Core Rule Set Fixes a Critical Security Bypass Vulnerability

Date: 7 January 2026
CVE: CVE-2026-21876

Crítica

Description

A critical vulnerability has been identified in the *OWASP Core Rule Set (CRS*), the most widely used rule set for Web Application Firewalls (WAFs) such as ModSecurity.

The flaw lies in the processing of multipart requests, allowing an attacker to bypass security rules by using specially crafted requests. This evasion may enable malicious payloads—such as SQL injection, XSS, or other web-based attacks—to go undetected and unblocked by the WAF.

Although the vulnerability does not directly result in code execution, it significantly reduces the defensive capability of the WAF, making it easier to carry out high-impact attacks against protected web applications.

Affected Products

The products affected by this vulnerability include:

- OWASP Core Rule Set (CRS)
- Versions prior to 4.22.0 (4.x branch)
- Versions prior to 3.3.8 (3.x branch)
- Any WAF integrating these CRS versions

Solution

It is recommended:

- Update to OWASP CRS version 4.22.0 or later (4.x branch).
- Update to OWASP CRS version 3.3.8 or later (3.x branch).

References

- cvedetails.com
- secalerts.co

TLP:WHITE

Events

Cyber Security & Cloud Expo Global 2026
4 - 5 February

A leading international event that brings together technology leaders, CISOs, cloud architects, and innovation executives to analyze the major trends in cybersecurity and cloud computing. The conference focuses on emerging threats, security in hybrid and multicloud environments, Zero Trust, AI applied to defence, regulatory compliance, and digital resilience. It combines strategic keynotes, real-world case studies, and a large exhibition area featuring the sector's main vendors.

Link

Hcon
6 - 7 February

H-C0N is a technical cybersecurity conference with a strong hacker DNA, focused on advanced research, ethical hacking, reverse engineering, red teaming, blue teaming, and both offensive and defensive security.It stands out for its hands-on approach, in-depth non-marketing talks, highly technical workshops, and a highly specialised community, making it a key meeting point for professionals who live cybersecurity from the inside, with a hands-on mindset and a continuous-learning spirit.

Link

EspañaSec Cyber Summit 2026
10 - 11 February

EspañaSec Cyber Summit is a high-level conference focused on the strategic vision of cybersecurity, aimed at senior executives, CISOs, and leaders responsible for risk, technology, and compliance.It approaches security as a business enabler, addressing topics such as governance, risk management, regulation, cyber-resilience, the impact of AI, and decision-making in complex environments. The event features top-tier speakers and a clear emphasis on leadership and strategy.

Link

Ondata Congress – Digital Forensics and Cyber Intelligence
18 February

The Ondata Congress is a well-established event in the field of digital forensics and cyber intelligence, aimed at technical professionals, law-enforcement personnel, analysts, and experts in digital investigation.The event delves into forensic analysis, incident response, cybercrime investigation, OSINT, and threat intelligence, combining technical rigour, real-world case studies, and a highly practical approach that makes it a national reference point in these disciplines.

Link

Resources

- ***Checklist* of Best Practices**

A current list of cybersecurity actions with an operational focus: identity controls, critical updates, verified backups, vendor controls... perfect as a checklist for quick inspections or internal audits.

Link

- **Global Cybersecurity Outlook 2025 – World Economic Forum (WEF)**

A strategic, global report examining how cybersecurity is evolving in response to emerging technologies, geopolitical tensions, and resilience challenges.It provides key insights into risks such as supply-chain dependencies, the increasing sophistication of attacks, and capability gaps between organisations, along with recommendations for leaders who must navigate this growing complexity.

Link

- **GCA Cybersecurity Toolkit (Global Cyber Alliance)**

A toolkit of practical guides to help assess your security posture, strengthen common controls, and access free solutions with a clear focus on internationally recommended baseline defences.

Link

Subscribe to RADAR

Powered by the cybersecurity NTT DATA team

es.nttdata.com