Issue 117 | August 2026

NTT DATA

Radar

The Cybersecurity Magazine

What We Encrypt Today May Be Decrypted Tomorrow

By Lluis Quiles Ardila

Every so often, the same headline resurfaces: quantum computing is on the verge of breaking digital security as we know it. The claim spreads quickly and leaves an unsettling question behind: are we building a technology that could ultimately undermine our own security? Today, the most advanced quantum computers operate with just over a hundred physical qubits: noisy, unstable and highly error-prone. Breaking the kind of RSA keys we commonly rely on would require thousands of stable logical qubits, supported by highly efficient error correction. That level of maturity has not yet been reached. Even the most optimistic forecasts place it around 2035.

The risk is not something for the future. It is already reaching back into the present. The logic behind “harvest now, decrypt later” is to intercept and store encrypted traffic today so it can be decrypted tomorrow. In practice, this means that any information that needs to remain confidential beyond the next decade is already exposed, from medical records to trade secrets. Organizations will have to migrate to post-quantum cryptography before the threat fully materializes.

And this cryptography is no longer a promise. It is becoming the standard. ML-KEM and ML-DSA are emerging as international benchmarks, with hybrid deployments already taking shape across VPNs, TLS and certificates. The United States has set 2035 as the target for federal adoption, while Europe is focusing on critical infrastructure before the end of the decade. The industry is also moving. NTT Research has introduced a Zero Trust security suite designed for post-quantum environments and has developed the first post-quantum transport system capable of switching cryptographic methods without interrupting communications.

However, looking at quantum technologies only through the lens of cryptography would mean seeing just one side of the challenge. That is why, at NTT DATA, we have built a value proposition that covers the four domains of quantum technologies: computing, including optimization, simulation and machine learning; sensing and metrology; quantum communications, including QKD; and post-quantum cryptography, from asset discovery to migration.

From a security standpoint, we must also remember that these algorithms will protect malicious actors too. Quantum-resistant encryption is dual-use: it will shield legitimate communications, but also criminal networks and illicit markets.The World Economic Forum, through its Quantum Computing Governance Principles, and UNESCO, through COMEST, are already working on principles such as transparency, accountability and the prevention of malicious use.

We are also entering a period of convergence between AI and quantum technologies. Every model trained on sensitive data expands the surface that needs to be protected. The same applies to every agent operating autonomously across corporate systems. Digital trust is becoming a data lifecycle challenge.

In this edition of Radar, we wanted to address what is already a reality: post-quantum cryptography, key management and data protection. We also look at the trends reshaping the quantum ecosystem, and the capabilities organizations should start building today. The challenge is both twofold and urgent: prepare and experiment.

Organizations must migrate before the threat becomes real, while also exploring quantum applications that can deliver tangible impact. The examples are already there: NTT DOCOMO reorganized the base stations of its mobile network in just forty seconds, a process that would have taken classical methods twenty-seven hours.

At NTT DATA, we have also seen this potential firsthand, helping one client optimize logistics management and another improve its predictive maintenance model. New drugs, more efficient materials and lower-energy networks are part of the other side of the story, and that story is already beginning.

Lluis Quiles Ardila
Managing Director

Ransomware, Third Parties and Unpatched Vulnerabilities: The Invisible Chain of Risk

Chronicle by Marta Gonzalez Martino

Between June and early July, several major incidents confirmed a trend cutting across sectors and countries: exposure is no longer defined solely by an organization's own systems. Reliance on third parties, shared infrastructure, delayed patching, credential abuse and the automation of attack stages all amplified the impact of breaches that, in many cases, began with a single vulnerable point.

Australia's second-largest sugar producer, Mackay Sugar, woke on 10 June to find its systems at a standstill. The company confirmed that it had suffered a cyberattack affecting two of its three main mills, forcing it to switch to manual processes to handle cane that had already been harvested. On 15 June, the group known as The Gentlemen, identified by Microsoft as Storm-2697, claimed responsibility for the attack. The actor operates under a RaaS model partly inherited from LockBit and uses a Go-based encryptor with worm-like lateral movement capabilities, as well as EDR evasion techniques through the GentleKiller framework. Mackay Sugar showed how the boundary between IT and OT is becoming increasingly porous.

Around the same time, Google Threat Intelligence and Mandiant disclosed a campaign targeting Oracle PeopleSoft, attributed to ShinyHunters. Between 27 May and 9 June, before Oracle published its security advisory on 10 June, the attackers exploited a zero-day vulnerability in PeopleSoft, software used to manage critical functions such as HR, finance and supply chain operations. According to Google, the attackers deployed MeshCentral agents disguised as legitimate cloud endpoints to run administrative commands.

On 22 June, Tata Electronics confirmed a cybersecurity incident affecting some of its corporate systems, after World Leaks published more than 200,000 files on the dark web, totalling over 630 GB of data. Reuters reported that the documents allegedly included designs, specifications, manufacturing files, emails, logs and passport copies, as well as material related to customers such as Apple and Tesla. Later details raised the stakes further: the leak included component and supplier lists, as well as material linked to testing of the unreleased iPhone 18 Pro. Following the incident, the company tightened internal controls, restricted remote access to sensitive tools, commissioned a forensic audit and notified authorities and customers.

On 23 June, attention shifted to Japan. KDDI Corporation, one of the country's major telecommunications companies, confirmed that it had detected unauthorized access to an email system serving six ISPs, including STNet, KDDI Web Communications, JCOM, Chubu Telecommunications, Nifty and BIGLOBE. The access was detected on 17 June and, according to KDDI, resulted from the exploitation of a vulnerability in third-party software integrated into that shared system. The potential exposure reached up to 14.22 million email addresses and passwords, including active, legacy and inactive accounts. KDDI stated that its mobile email system was not affected, but the incident left a clear lesson: the domino effect. A vulnerability in shared infrastructure can become a single point of failure for several providers at once.

By late June, attention had shifted to a more uncomfortable area: credentials, unpatched systems and attack automation. BlueHammer, a Windows Defender vulnerability flagged by CISA as being actively exploited in malware and ransomware campaigns, had already been patched by Microsoft in April. The flaw allowed attackers to escalate privileges to SYSTEM through a race condition.

In early July, JadePuffer emerged as a particularly relevant case for understanding attack automation. Sysdig Threat Research Team described it as the first known case of agentic ransomware: an extortion operation automated through an agent powered by a language model. Initial access was achieved by exploiting CVE-2025-3248, a critical vulnerability in Langflow that allows arbitrary code execution without authentication on exposed instances. From there, the agent automated reconnaissance, credential discovery, data extraction and lateral movement into internal services. According to Sysdig, the attack ultimately reached a Nacos platform, where more than 1,300 configuration items were encrypted and a ransom note was left behind.

On 1 July, Spain entered the sequence with Indra, which confirmed that ransomware had been detected in one of its subsidiaries. Its CSIRT activated analysis, containment, eradication and recovery protocols. According to the company, the incident was limited to a non-critical environment, did not spread to the rest of the group and did not disrupt service delivery. The attack was claimed by The Gentlemen, which listed Indra on its leak site with a countdown before the publication of allegedly stolen data, although neither the exfiltration nor the type of information affected had been publicly confirmed.

On 5 and 6 July, another case emerged with a different shape but the same underlying theme: FortiBleed. According to reports published by The Times and The Sun, attackers linked to Russia allegedly used vulnerabilities in Fortinet firewalls, combined with brute-force techniques and previously leaked credentials, to access accounts belonging to UK public bodies. Reported victims included Foreign Office personnel, local government employees and technical staff at British embassies in Thailand and Mauritius. The NCSC confirmed a brute-force campaign and urged organizations to review their credentials and configurations.

Taken together, these incidents point to a clear conclusion: the attack surface no longer ends at an organization's internal systems. It now extends across suppliers, shared platforms, SaaS integrations, reused credentials, exposed firewalls, unpatched vulnerabilities and tools that, if left unmanaged, can become the first link in a much larger intrusion.

Mackay Sugar showed how a digital attack can disrupt physical operations. KDDI exposed the risk of shared infrastructure. PeopleSoft and Tata Electronics highlighted the weight of the supply chain. BlueHammer and FortiBleed served as a reminder that known but unpatched issues remain exploitable. JadePuffer added attack automation as a new layer of pressure. And Indra showed that even a contained incident can be significant when the victim operates in strategic sectors.

Marta Gonzalez Martino
Cybersecurity Consultant

Post-Quantum Security: Entering the Age of Crypto-Agility and Crypto-Resilience

Article by Kim Boermans

Quantum computing is moving beyond the research lab and beginning to establish itself as a strategic force with real-world impact. One of the areas it is set to transform is cybersecurity, particularly because of its potential to challenge the cryptographic foundations that underpin the digital economy.

Today's encryption model rests on a basic assumption: that certain mathematical problems are practically impossible to solve with the computing power currently available. Quantum computing is beginning to challenge that assumption. In time, it could render widely used algorithms such as RSA and ECC obsolete, dramatically reducing the time needed to break them.

This is no longer a distant concern. The concept of "harvest now, decrypt later" means that data captured today could be compromised once quantum technology reaches maturity.

Organizations need to act early and gain full visibility into where and how cryptography is used across their digital ecosystems. This means assessing legacy systems, distributed architectures and data that, due to regulatory requirements, must remain secure for years or even decades.

Towards a Quantum Security Roadmap

The transition to post-quantum security requires a sustained strategy that brings together technology, processes and organizational capabilities. There is no switch to flip, and no silver bullet that can solve the problem overnight.

Along the way, two key capabilities need to be developed. The first is crypto-agility: the ability to adapt dynamically to new standards without disrupting business operations, while prioritizing actions effectively.

Essential first steps include identifying cryptographic assets, mapping dependencies and understanding which data is at risk. From there, organizations can design a roadmap to support the transition to quantum-resistant algorithms, together with more efficient and scalable management models.

The second capability is crypto-resilience: the ability to respond quickly to emerging vulnerabilities, maintain regulatory compliance and preserve trust in a constantly evolving environment.

Convergencia con tecnologías emergentes

The convergence of quantum technologies with other emerging fields, such as artificial intelligence, digital twins and blockchain, is expanding both the opportunities and the security requirements. Data used to train models, optimize operations or simulate scenarios must remain protected, even while it is being processed. This raises the bar for the level of protection organizations need to provide.

As a result, more comprehensive approaches are emerging, combining strategic advisory, applied experimentation and phased implementation models. Assessing technologies, building prototypes and validating specific use cases can help reduce uncertainty and accelerate adoption with lower risk.

At the same time, the shift towards cryptography-as-a-service models is changing operational dynamics. These models centralize capabilities, automate key management and continuously adapt algorithms without disrupting business operations.

This approach strengthens security, simplifies operations, reduces costs and enables more agile responses. Quantum computing opens the door to new levels of optimization and efficiency across multiple industries. However, capturing that value requires building a solid foundation of digital trust today. The process starts with a simple question: which cryptographic algorithms are protecting our most valuable data, and how exposed will they be in a quantum future?

Kim Boermans
Head of Cybersecurity NTT DATA Benelux & France

Seven Trends Reshaping the Quantum Science and Technology Ecosystem

Trends by María Gutierrez

For years, the conversation around quantum technologies has focused almost exclusively on quantum computing. But the real shift is much broader. The so-called second quantum revolution is giving rise to an ecosystem that brings together computing, communications, cryptography, algorithms, sensing and metrology, with strategic implications for industry, security and competitiveness. These are the key trends that we believe will shape its evolution in the years ahead:

1. From Qubit Count to Useful Performance. The industry has moved beyond the race to increase the number of qubits as the main measure of progress. The focus is now shifting to metrics such as operational reliability, error correction, architectural scalability and the ability to run algorithms that deliver practical value. At the same time, the sector is advancing through the so-called NISQ era, or Noisy Intermediate-Scale Quantum, defined by devices with a limited number of qubits that are still affected by noise. The challenge is no longer just to build larger processors, but to develop quantum systems that are reliable, scalable and genuinely usable.

2. Quantum Sensing Moves First into Commercial Use. While quantum computing continues to mature, quantum sensors are emerging as the technology most likely to deliver impact in the near term. Their exceptional sensitivity could improve navigation without relying on GPS, strengthen the monitoring of critical infrastructure, support geological exploration, advance biomedical diagnostics and enable Earth observation with unprecedented precision.

3. Metrology: The Quiet Enabler of the Digital Economy. Advances in optical atomic clocks and quantum interferometry are redefining the standards for measurement and synchronization. These capabilities will be essential for smart power grids, advanced telecommunications, financial systems, precision navigation and future 6G infrastructure, where timing accuracy will become a strategic asset.

4. Quantum Communications Move Towards Secure Infrastructure. Quantum key distribution, or QKD, metropolitan quantum networks and the first experiments with quantum repeaters are laying the foundations for a future quantum internet. Significant technological challenges remain, but many countries already see these capabilities as critical infrastructure for protecting government, financial and defence communications. They are also set to become one of Europe's major priorities in the years ahead.

5. Post-Quantum Cryptography Moves from Research to Planning. The standardization of new algorithms designed to withstand quantum attacks marks the start of a transition that will affect every organization. The challenge is not only technological, but also organizational: identifying critical assets, planning the migration and ensuring the protection of information whose lifecycle may span decades. This is one of the most immediate priorities. In fact, we could say it is no longer just a trend — it is becoming a mainstream imperative.

6. Artificial Intelligence Accelerates Quantum Development. The convergence of AI and quantum technologies is one of the most promising trends in the field. AI is already being used to optimize materials design, support the experimental control of quantum devices and calibrate sensors. In the medium term, quantum computing could also enhance certain optimization and machine learning algorithms.

7. Competitive Advantage Will Depend on the Ecosystem, Not Only on the Technology. International competition is no longer limited to hardware development. Europe, the United States and China are deploying strategies that combine public investment, industrial collaboration, talent development, standardization and research infrastructure. For companies, the challenge is to identify use cases, build internal capabilities and take part in these ecosystems before the technology reaches full maturity.

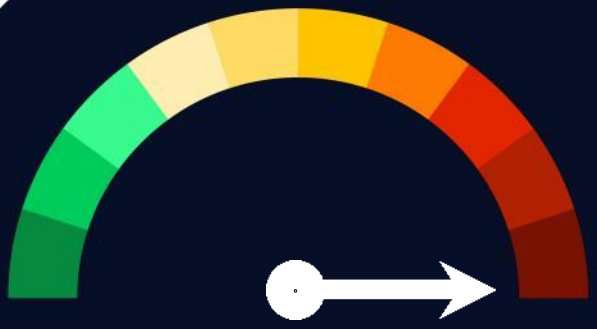
Quantum science and technologies are no longer a distant promise. They have become a strategic pillar of industrial and innovation policy. Adoption will be gradual and uneven, but organizations that start building knowledge, partnerships and capabilities today will be better positioned to capture the value of a technological revolution that is already underway.

María Gutierrez
Cybersecurity Expert

Vulnerabilities

Google Chrome Sandbox Escape

Date: June 30, 2026
CVE: CVE-2026-13782



CVSS: 10
CRITICAL

Description

CVE-2026-13782 is a critical vulnerability caused by a Use-After-Free error (CWE-416) in the Chrome browser, where memory is reused or referenced after it has been released.

In this scenario, an attacker who has previously compromised the renderer process could exploit this error to escape the Chrome sandbox through a specially crafted HTML page.

This type of vulnerability is particularly critical because the sandbox is one of the browser's main security barriers, which is why it has a CVSS score of 10.

Solution

It is recommended to:

- Update Chrome to version 150.0.7871.47 or later.
- Keep automatic updates enabled

Affected Products

- Google Chrome for Windows, Linux or macOS versions prior to 150.0.7871.47.

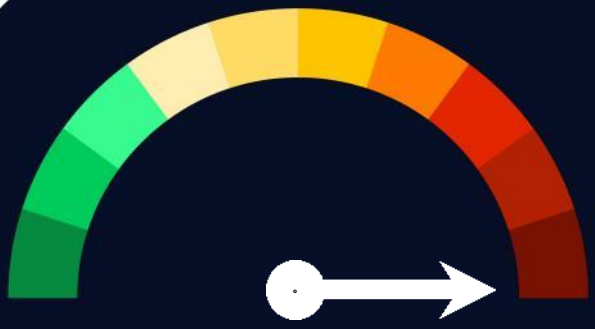
References

- nvd.nist.gov
- rapid7.com
- incibe.es
- cvedetails.com

Vulnerabilities

Adobe ColdFusion Path Traversal

Date: June 30, 2026
CVE: CVE-2026-48282



CVSS: 10
CRITICAL

Description

Adobe ColdFusion is affected by a path traversal vulnerability in the Remote Development Services (RDS) component. This flaw allows an unauthenticated attacker to manipulate file paths sent to the server through HTTP requests, enabling them to break out of the permitted directories and access arbitrary locations on the system. It could also allow the attacker to write malicious CFML (ColdFusion Markup Language) code to directories accessible by the web application, potentially leading to remote code execution.

The root cause lies in ColdFusion's failure to properly validate and restrict user-supplied file paths in certain RDS service operations.

Solution

It is recommended to:

- Update to ColdFusion 2025 Update 10 and ColdFusion 2023 Update 21.

Affected Products

- ColdFusion 2025 Update 9 and earlier.
- ColdFusion 2023 Update 20 and earlier.

References

- adobe.com
- nvd.nist.gov
- sentinelone.com
- cvereports.com

BMC Security Patch for a Critical Control-M/Server Vulnerability

Date: July 1, 2026
CVE: CVE-2026-10539

Critical

Description

Due to insufficient command validation, vulnerability CVE-2026-10539 could allow an unauthenticated remote attacker to execute unauthorized commands on the Control-M/Server, potentially enabling lateral movement within the infrastructure.

Control-M is a workload automation scheduler widely deployed in large organizations across telecommunications, banking, insurance, public administration and industry. For this reason, the potential impact of this vulnerability is high, as it could compromise a system that supports multiple business processes and dependent systems.

Affected products

The affected products are:

- Control-M/Server from version 9.0.20.x up to and including version 9.0.21.200.

Solution

It is recommended to:

- Update Control-M/Server to version 9.0.21.300 or later.
- Restrict access to Control-M/Server to trusted networks only.

References

- incibe.es
- nvd.nist.gov
- bmcapps.my.site.com

BeyondTrust corrige múltiples vulnerabilidades en Remote Support y Privileged Remote Access

Date: July 6, 2026
CVE: CVE-2026-40138 y 3 más

Critical

Description

BeyondTrust has addressed multiple vulnerabilities affecting BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA), two products used for remote access, remote support and privileged access management.

These vulnerabilities could allow an unauthenticated attacker to bypass access controls, gain unauthorized access to the system or cause a denial of service.

In addition, one of the vulnerabilities could allow authenticated users with limited privileges to access resources or data beyond their authorized scope. The risk is particularly relevant in environments where these solutions are exposed to a network or the internet.

Affected products

The affected products are:

- BeyondTrust Remote Support (RS) version 25.3.2 and earlier.
- BeyondTrust Privileged Remote Access (PRA) version 25.3.2 and earlier.

Solution

It is recommended to:

- Update the products to version 25.3.3.
- In environments where an immediate update is not possible, apply the April 2026 Security Rollup.

Refrences

- beyondtrust.com
- thehackernews.com
- nvd.nist.gov
- cybersecuritynews.com
- csirt.telconet.net

Events

Black Hat USA 2026
August 1–6

The year's leading cybersecurity event returns to Mandalay Bay with a redesigned six-day program created to drive innovation, push boundaries and bring the global security community together like never before.

This year's edition will feature four days of expert-led immersive training from August 1 to 4, followed by Summit Day on Tuesday, August 4, and a two-day main conference with cutting-edge briefings, open-source tool demonstrations at Arsenal, a dynamic Business Hall, and multiple opportunities for learning and networking.

Link

DEF CON 34
August 6-9

DEF CON is the world's largest and longest-running hacker conference, known for its "village" model, where communities of interest organize hands-on workshops and talks. The DEF CON Car Hacking Village is a key meeting point for automotive security researchers, featuring live vehicle hacking demonstrations, CTF competitions focused on real automotive systems, and talks on the latest vulnerabilities affecting connected vehicles.DEF CON is also where many major discoveries in automotive security are revealed for the first time.

Link

SANS Security Awareness & Culture Summit 2026
August 19-28

This is the 13th edition of the summit, focused on professionals working in cybersecurity awareness, human behavior and security culture. The event is designed to share knowledge, experiences and practical tools to help drive meaningful change in organizations' security cultures.

The program includes expert talks, use cases, hands-on sessions and in-person workshops, with a focus on how to influence not only employee behaviors, but also their attitudes and beliefs towards cybersecurity. It also offers networking opportunities with experts and other professionals from the sector.

As a complement, SANS also offers related courses on cybersecurity leadership and human risk management, designed to strengthen capabilities in awareness, training and cultural change programs. It is a particularly relevant event for organizations looking to move beyond one-off awareness campaigns towards more mature Human Risk Management models.

Link

Resources

➢ Cyber Frontier 2026

NTT DATA's annual publication brings together insights from cybersecurity experts, researchers and professionals. The 2026 edition explores topics such as the talent gap, breach defence, AI-driven disinformation threats and preparation for the disruption caused by quantum computing.

Link

➢ Verizon 2026 Data Breach

One of the most widely recognized reports on security breaches and real-world incidents. The 2026 edition provides insights into how organizations can respond to AI-enabled attacks, financial pressure, ransomware, vulnerabilities and sector-specific risks.It also includes an executive summary, infographics and industry-specific resources.

Link

Subscribe to RADAR
up.nttdata.com/suscribetearadar

Powered by the cybersecurity NTT DATA team

es.nttdata.com