Number 104 | July 2025

NTT DATA

Radar

The Cybersecurity magazine

Data Security: the new digital, intelligent, and regulated perimeter.

By Jorge Trujillo Ramírez

Today, the rules of the game have changed. In a data-driven economy, we can no longer focus solely on protecting static databases or preventing phishing attacks. Data security now lies at the heart of a radical transformation, driven by the widespread adoption of emerging technologies such as Artificial Intelligence (AI), distributed cloud, industrial IoT, and machine learning. In this new environment, protecting data is not just a technical or compliance matter—it's a question of cross-sector strategic leadership. Cyberattacks don't discriminate based on size or type of organization. So far this year, security breaches have cost billions to organizations that, paradoxically, were already investing millions in infrastructure.

Emerging Technologies: New Assets or New Risks?

The use of generative AI, robotic automation, connected devices, and digital twins is transforming sectors such as healthcare, industry, banking, and insurance. However, these technologies have also significantly expanded the attack surface.

- **In the healthcare sector:** AI used in clinical diagnostics processes sensitive data in real time. Any data breach could have serious ethical, legal, and reputational consequences.
- **In the banking and insurance sector:** risk scoring algorithms handle personal and financial data that must comply with GDPR, DORA, and local regulations.
- **In the industrial sector:** IoT sensors and SCADA networks generate critical industrial data, often lacking proper segmentation and native cloud protection.

The very technologies that drive efficiency also introduce new and significant risks.

A New Regulatory Landscape

Organizations now face the challenge of operating in an increasingly demanding and exposed regulatory environment. Regulatory frameworks are shifting from a "should have" approach to a "must prove" one. In other words, it's no longer enough to have controls in place — continuous evidence of their effectiveness is now required. Examples of this shift include:

- **DORA (*Digital Operational Resilience Act*):** Requires banks and insurance companies to manage third-party risks, ensure business continuity, and conduct cybersecurity testing.
- **NIS2 (UE) and LATAM versions:** amplían el concepto de infraestructura crítica, incluyendo salud, minería, tecnología y energía.
- ***AI Act, Executive Orders, GDPR, LGPD, and their local equivalents*:** Establish clear accountability for automated decisions and the ethical use of data.
- **New sector-specific standards (such as IEC 62443, NIST, HITRUST):** These are now integrated as requirements in audits and procurement processes.

Protected Data Means Protected Business

Organizations that understand data is no longer the sole responsibility of IT departments—and instead view it as a strategic asset rather than just a risk—are focusing their investments on three key fronts:

1. **Data Governance:** Knowing what data exists, where it resides, and who has access to it.
2. **Security Culture:** Training all staff, not just the IT team, to adopt secure behaviors.
3. **Proactive Regulatory Risk Management:** Turning compliance into a market advantage by anticipating regulations and embedding them into business processes.

And this is where **IT leaders (CISO, CTO, CIO)** must take action:

- Designing secure architectures, incorporating responsible use of Generative AI and data—across both cloud and OT environments.
- Properly adopting autonomous security technologies, such as AI-powered EDR, UEBA, and DLP-as-a-service.
- Aligning and reinforcing cybersecurity culture with overall business strategy.
- Integrating cybersecurity, compliance, and data governance into a unified model.

Conclusion:

Each day, an organization's value is increasingly tied to its ability to protect, govern, and use data in an ethical, responsible, and trustworthy manner. That's why organizations that fail to see data protection as an extension of business protection will struggle to succeed in a world where compliance alone is no longer enough—leadership must be built on trust.

Jorge Trujillo Ramírez
Cybersecurity Project Leader

Attacks on “giants” caused by small “mistakes”

Cyber Chronicle by Aldemar Moreno Moreno

Nowadays, it is striking to see major corporations—many of which have migrated their workloads to well-known cloud providers—suffer data breach incidents. This happens despite having made significant investments in cybersecurity solutions, employee training, assurance processes, and continuous evaluation and monitoring of these platforms.

What companies like Delta Airlines (Threat Actor: MoveIT – Supply Chain Attack), Toyota (Criminal Group: Medussa – Cause: lack of patches), or NPD - National Public Data (Criminal Group: USDoD – Cause: website vulnerabilities) have in common—just to name a few examples—is the disclosure of exposed sensitive data. The preventive and protective measures for these exposures are outlined in various security assurance frameworks and are everyday tasks within cybersecurity teams.

It’s not that the attackers used sophisticated techniques to gain access, encrypt, and/or exfiltrate that information. On the contrary, they relied on techniques that are easy to learn by someone with an intermediate level of technology knowledge, using tools available to anyone. Let’s look closely at a recent example.

Let’s talk about the CodeFinger ransomware that affects buckets on AWS. Unlike other attacks such as the one that impacted Delta Airlines, directly affecting a secure data transfer solution in the supply chain—MoveIT (an attack we covered in the October 2024 cyber report)—CodeFinger relatively easily breaches exposed information on the S3 service
Todo comienza con una simple enumeración de *access key* expuestos, o claves previamente comprometidas.

Using dorks such as: "AWS_SECRET_ACCESS_KEY" OR "aws_access_key_id" site:github.com and being a bit more specific with the input parameters, extensive examples of secret exposures can already be obtained to proceed with the next step. Even using tools like Shodan, GitGuardian, or other resources, data is often gathered to design and refine the attack profile. At this point, the attacker can verify whether the obtained keys have the permissions “s3:GetObject and s3:PutObject,” in which case they proceed to the next step:

- Enumerate the S3 buckets and objects to determine if there is any specific interest in the information that could increase the ransom demand.

- Once the data is identified, the next step is to encrypt it using SSE keys with AES-256 symmetric encryption keys. At this stage, the generated keys are stored by the attacker, preventing the resource administrator from regenerating them to try to recover the information. The most they can see are logs in CloudTrail, the creation of keys, and an ID with which nothing can be done regarding recovery.

- Finally, the data lifecycle is modified by adjusting its retention policies so that if the ransom is not paid, the encrypted data is deleted. The cherry on top is the personalized ransom message that we all know, including the respective Bitcoin account for payment, as well as terms and conditions.

Since this attack is recent, the names of affected companies have not yet been disclosed, and it is possible that for several months they will remain unaware while the attacker silently carries out identification, encryption, and refinement of the attack.Now, when we talk about simple or at least well-known measures, it is necessary to refer to the different assurance frameworks. Among the measures included in the CIS Benchmark for AWS or Azure, NIST Cybersecurity Framework, Cloud Control Matrix by CSA, Azure Security Benchmark, AWS Well-Architected Framework, among others, provide a detailed compendium of controls and specific configurations for data protection. To continue focusing on prevention measures against CodeFinger, CIS itself indicates the following:

- **Use short-term access keys:** preferably linked to IAM (Identity and Access Management) and AWS STS (Security Token Service) with short-term access.
- **Restrict** the use of SSE-C via IAM policies to prevent unauthorized users from using it and enforce specific conditions (for example, only from allowed IPs, or for short periods, etc.).
- **Enable** versioning and object lock to prevent overwriting or deletion of critical data.
- **Monitor and audit key usage in AWS:** this includes periodic review of permissions, expiration, and service scope. Services like GuardDuty provide intelligence and analytics to easily detect when a threat may be materializing.
- **Enable activity logging:** through CloudTrail and linked to GuardDuty (or the organization's intelligence and data analysis system). The more detailed, the better, as it allows gathering and providing unusual patterns to intelligence tools, such as mass encryption or changes in data retention policies.

The above measures are usually easy to implement and represent the ABC of cybersecurity operations in this type of infrastructure. However, we see that their application, compliance evaluation, posture analysis, monitoring, and alerting are not being properly carried out, even in large corporations. What can we think about the assurance conditions in SMEs or organizations with little awareness of data security?

We must start with basic assurance, but we also need to prepare for the challenges posed by attacks using quantum computing — more sophisticated, faster, and more efficient. Against these, basic assurance protocols will no longer be enough; we must consider new protection mechanisms.

In the case of AWS, Kyber is already being discussed for more secure key management, post-quantum TLS for secure connections, and Kyber in SSH for protecting data in transit. Azure is also incorporating ML-KEM in Storage, KeyVault solutions, and those using TLS 1.3. Both AWS and Azure align with NIST's FIPS 203 publication (which is highly recommended reading to understand the implications of this new technological challenge). In cybersecurity, the key is to follow existing leading practices, study trends, never underestimate the opponent, and carefully read the cyber chronicles.

Aldemar Moreno Moreno
Cybersecurity Consultant

Differential Privacy, a hidden yet essential control in analytical data protection models

Article by Jaime Tovar Prieto

Although data and information security have always been a general concern, many people feel reassured when they hear the statement “We protect your information,” yet few seek to understand how this is achieved. In light of this, this RADAR article will address the concept of Differential Privacy, used by industry giants like Google, Apple, and Microsoft, which underscores its effectiveness in protecting information.

What is Differential Privacy?

Differential Privacy is a mathematical framework designed to protect data privacy. It allows analysis on large datasets without revealing sensitive information about individuals by adding "noise" to the results. This approach ensures that the overall outcome remains accurate while personal or sensitive information stays hidden.

The mathematical model applied to the data seeks to extract useful insights and perform statistical analysis on datasets that may contain sensitive information (such as personal data, beliefs, health, religion, or corporate secrets), reducing the risk of data exposure and safeguarding responsibilities through due diligence, in compliance with relevant regulations on data collection and processing.

The application of this security model aims to tangibly balance the need to obtain insights from analyzing large volumes of data (Big Data) with the ethical responsibility to protect information privacy.

Its origins

The basis of this concept dates back to 1977, when Tore Dalenius proposed the possibility of extracting specific information from a database without revealing details about an individual. In 2006, Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith established that, in many cases, it is possible to obtain highly accurate information while simultaneously ensuring a high level of privacy.

Is Obfuscation the Same as Differential Privacy?

From a superficial point of view, one might consider them the same; however, they are not.

While traditional approaches aim to anonymize data used in analytical models, Differential Privacy focuses on limiting the amount of information exposed that could be inferred or linked to an individual.

Conventional models can be inefficient; although effective in certain scenarios, they can be vulnerable to re-identification attacks. For such an attack to be successful, an additional vector related to obtaining extra information is needed. An example occurred in 2015, when researcher Latanya Sweeney, in her work “Only You, Your Doctor, and Many Others May Know,” identified 43% of patients in a medical data report from the state of Washington, demonstrating that obfuscation processes are only partially effective for protecting information

So, how does it work?

As mentioned earlier, Differential Privacy is based on a mathematical model, specifically on the parameter epsilon (ε) and, in some cases, delta (δ). Epsilon represents the privacy budget, a number defining the level of noise added to a dataset. A smaller epsilon value indicates a higher level of protection but sacrifices some accuracy in the analysis, while a higher value allows more precision but less data protection.

Delta reflects the probability that the privacy guarantee might fail or be compromised beyond what epsilon defines. Delta is a very small number, close to zero (for example, 10^-5, which equals 0.00001). It is important to note that the presence of this variable may enable, to some extent, the possibility of information leakage but, in return, allows for improved results in certain cases.

A fundamental property of this mathematical model is that the algorithm's results should be the same regardless of whether a particular individual's data is included or not in the dataset.

The first key concept in **Differential Privacy** is the addition of noise, which involves inserting random data into the original dataset, making it difficult to identify the influence of any specific data point on the final result. Two main models are considered for the injection or addition of noise:

- **Laplace Mechanism:** adds random noise following a Laplace distribution, which has a peaked shape and is sensitive to changes. This mechanism is used for publishing demographic or medical data.
- **Gaussian Mechanism:** adds random noise following a Gaussian distribution, which has a bell-shaped curve and is suitable for protecting large volumes of data.

Additionally, there are other mechanisms within **Differential Privacy** that do not add noise, such as:

- **Randomized Responsed:** introduces randomness in answers to sensitive questions.
- **Data Perturbation:** modifies the original dataset by intentionally altering some values.

However, Differential Privacy has some points that require attention, including:

- Complexity in implementation
- Impact on small datasets
- Implementation error

Industry Applications

Google applies this privacy model to gather information from several of its products, such as search results on Android devices and the use of Google Cloud BigQuery. The latter is a clear example of this security component, as it allows adding noise to results to protect confidentiality.

Apple uses device analytics to collect data on product usage, such as keystrokes, errors, and emoji usage. This data collection is processed in a way that limits the total number of contributions a user can make, preserving their privacy over time..

Conclusion

In summary, **Differential Privacy** is an essential control in data collection and ingestion, as it allows generating useful results without exposing information about individuals. Its application not only protects privacy but also establishes an ethical standard that must be considered when handling personal data in the digital age.

Jaime Tovar Prieto
Cybersecurity Architect

The Quantum Port: How Logistics Is Beginning to Benefit from Quantum Computing

Quantum Space by María Gutiérrez

Although quantum computing has not yet reached a level of maturity for widespread deployment in real production environments (mainly due to limitations of quantum hardware), significant advances are already being made in sectors where optimization problems are particularly complex. It's not just about simulating molecules or breaking cryptography; other fields are already benefiting from this technology, such as logistics—especially port logistics—with thousands of containers moving daily, critical decisions needing to be made in seconds, and multiple operational constraints.

Ports are becoming ideal scenarios to test quantum algorithms. The Port of Los Angeles, one of the largest and most congested ports in the world, has been at the forefront of one of the most notable use cases to date.

One of the first real experiments applying quantum computing to port logistics was made possible by the collaboration between SavantX, a company specialized in predictive analytics, and D-Wave Systems, a pioneer in quantum annealing—a specialized form of quantum computing designed specifically to solve combinatorial optimization problems, extremely efficient for problems involving finding the minimum or maximum of a function with many interrelated variables.

The challenge was to find the best way to rearrange containers so cranes could locate them faster. This challenge grows in complexity as the number of elements increases, soon becoming impractical for classical computers. The result? According to project leaders, a 60% improvement in operational efficiency was achieved—meaning fewer unnecessary movements, less waiting, less chaos, and lower costs. The message was clear: quantum computing can make a real difference in complex scenarios.

The port case is not the only one; other companies are beginning to explore how quantum algorithms can help them in their supply chains. For example, in optimizing taxi routes during high-demand events, solving planning problems in factories where issues such as optimal component assembly and dynamic inventory management are tackled. Also, in the financial sector for portfolio optimization, fraud detection, and derivative valuation.Although current quantum computers have significant limitations (they are sensitive, require extreme cooling, and do not yet have the scale needed to solve massive problems), experiments like those conducted at the port help pave the way and teach how to integrate these new approaches with classical systems. Meanwhile, large companies are working to build more powerful, stable, and accessible quantum computers.

If progress continues at this pace, many of the algorithms currently being tested in laboratories could start running in production before the end of this decade, because in a world where every second counts and every route can be optimized, quantum computing is beginning to stop being just a promise.

The port case is just one example of how these technologies can start solving present-day problems. We might not see a 100% quantum global logistics network tomorrow, but the first steps have been taken... among containers...

Seguridad de los datos en la época cuántica

Article by Cesar Huanayque Vilca

While quantum computing promises to revolutionize numerous fields—from medicine to materials science—it also poses an existential threat to the foundations of today's digital security. Cryptographic algorithms that protect global communications and data, such as RSA and ECC, are vulnerable to attacks by sufficiently powerful quantum computers. In response, Post-Quantum Cryptography (PQC) is emerging as the essential countermeasure, offering a new generation of algorithms that are resistant to these future threats and ensuring the confidentiality of our information in the upcoming technological era.

What is Post-Quantum Cryptography (PQC)?

PQC refers to the development of cryptographic algorithms that are secure against attacks from both classical computers and future quantum computers. Unlike quantum cryptography, which uses quantum physics for security, PQC relies on mathematical problems that are believed to be intractable even for a quantum computer.

One of its main advantages is that these new algorithms are designed to be implemented within existing classical IT infrastructures, making the transition easier and protecting us against the immediate threat of "Harvest Now, Decrypt Later" (HNDL) attacks, where adversaries collect encrypted data today with the intention of decrypting it in the future when quantum technology becomes available

NIST Standardization

The U.S. National Institute of Standards and Technology (NIST) has led a global effort to standardize robust and reliable PQC algorithms. After an evaluation process that began several years ago, in August 2024, NIST announced the completion of the first official PQC standards:

- **FIPS 203 (ML-KEM):** lattice-based key encapsulation mechanism (CRYSTALS-Kyber) for secure key establishment.
- **FIPS 204 (ML-DSA):** a lattice-based digital signature algorithm (CRYSTALS-Dilithium) for authentication.
- **FIPS 205 (SLH-DSA):** a hash-based digital signature algorithm (SPHINCS+), offering a robust alternative.

The process continues with additional algorithms such as **FALCON** and **HQC** (a code-based KEM selected in March 2025), aiming to diversify the available cryptographic defenses.

Data Protection Strategies in the Quantum Era

PQC must be applied across all data states to ensure comprehensive protection:

1. **Data in transit:** Communications (VPN, TLS, etc.) must be updated to use PQC algorithms, such as ML-KEM for key exchange and ML-DSA for digital signatures, thereby ensuring confidentiality and authenticity.
2. **Data at Rest:** Stored data is encrypted with robust symmetric algorithms (like AES-256), but the keys protecting this data must be encrypted or "wrapped" using a post-quantum KEM.
3. **Data in use:** Protection here is more complex, but many modern Homomorphic Encryption schemes (which allow computations on encrypted data) are already based on lattice problems, making them inherently quantum-resistant.

Finally, the transition to Post-Quantum Cryptography is not a simple technological upgrade—it is a fundamental strategic evolution for long-term security. Although "Q-Day"—the moment a quantum computer can break current cryptography—is uncertain, the threat of "Harvest Now, Decrypt Later" is present and real. Organizations that begin their journey toward quantum resilience today will not only protect their most valuable assets but also build a stronger and more enduring foundation of digital trust for the future.

Cesar Huanayque Vilca
Cybersecurity Expert Architect

How does the evolution of a user's digital footprint affect a company's security posture?

Trends by Shirley Villacorta Aristondo

Over the past five decades, the way we know and connect with people has evolved drastically. Until recently, establishing meaningful connections depended on our interpersonal skills: "talking, speaking, and observing." These methods, combined with genuine interest and creativity, facilitated relationships where each interaction revealed surprises and nuances, without the immediacy that characterizes communication today.

However, over the past decade, we have experienced a radical shift in our interpersonal behaviors. Talking and observing have become somewhat "vintage." Now, our interactions are predominantly focused on the information we choose to share in the digital environment, fostering a more analytical approach. This new dynamic includes searching for information about people's identities and digital footprints, combined with an intuitive use of OSINT (Open Source Intelligence), which broadens our ability to understand others.

Today, we face an even more complex and challenging landscape, driven by the explosion of Artificial Intelligence (AI). The use of AI has radically reshaped how we interact and get to know each other. Thus, the knowledge we gain about a person increasingly comes from their digital footprint and the inferences AI can draw from data about behaviors, emotions, and even psychological traits. In this way, we become digital representations, the result of predictive algorithmic analysis.

Presentation of New Threats

In this context, it is urgent to reflect on the need to develop effective proposals for data protection and identity and privilege governance. With the increased use of algorithms and AI to interpret our characteristics and behaviors, legitimate questions arise about privacy, consent, and personal information security. New threats have emerged in the corporate environment, such as deepfakes, biometric identity cloning, and account takeover through advanced BEC (Business Email Compromise).

Collaboration in the New Security Posture So, how can we contribute to redefining the information security posture in companies? We can focus on three key areas:

- **New Protection Perimeter:** The protection framework has shifted, with the user becoming the new perimeter. This enables the Zero Trust approach based on identity.
- **Digital Identity as a Corporate Risk:** Our employees' digital footprints have become a new target for attackers, who now have greater resources for profiling and carrying out successful cyberattacks. Adoption of Digital Risk Protection and Identity Threat Detection and Response solutions is expected to solidify between 2025 and 2026.
- **Privacy and Security as a Unified Front:** Privacy and security must work together as one. There will be no room for security postures that ignore privacy, or vice versa. The stable implementation of Privacy by Design and Security by Design will require security architecture models and the use of Data Discovery tools.

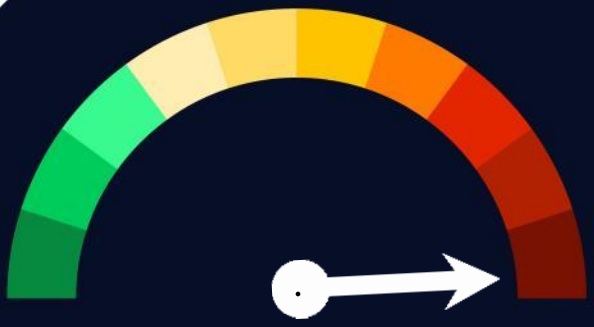
The era of systemic digital risk and the cybersecurity challenges it brings demand a proactive and ethical approach to information management. As we move toward a digital future, it is imperative to respect regulations and individual rights. In this context, cybersecurity is no longer just about protecting systems; cybersecurity programs must also protect people and their digital representations, as these have become the new perimeter that must be safeguarded.

Shirley Villacorta Aristondo
Cybersecurity Manager

Vulnerabilities

Critical Authentication Bypass Vulnerability in Fortinet

Date: May 28, 2025
CVE: CVE-2025-22252



CVSS: 9.8

CRITICAL

Description

This vulnerability, identified as CVE-2025-22252, is an authentication bypass that allows a remote attacker to gain administrative privileges without valid credentials.

This flaw jeopardizes the integrity and availability of affected systems by enabling full control takeover, modification of sensitive configurations, and potential theft of confidential information.

Due to its severity, with a CVSS score of 9.8, it represents a critical threat to organizations relying on these devices within their network infrastructures.

Solution

Fortinet released official patches between late May and early June 2025 that fix this authentication bypass.

It is recommended to update to the following versions:

- FortiOS 7.4.7 or higher
- FortiProxy 7.6.2 or higher
- FortiSwitchManager 7.2.6 or higher

Additionally, as a temporary measure, it is advised to restrict administrative access through firewall policies and strengthen access monitoring.

Affected Products

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

- FortiOS (7.4.4 a 7.4.6 and 7.6.0)
- FortiProxy (7.6.0 to 7.6.1)
- FortiSwitchManager (7.2.5)

Reference

- incibe.es
- fortiguard.fortinet.com

Vulnerabilities

High-severity vulnerability in Google Chrome

Date: June 2, 2025
CVE: CVE-2025-5419

CVSS: 8.8

HIGH

Description

A high-severity vulnerability has been detected affecting Google Chrome version 8.

This vulnerability could allow an attacker to exploit an out-of-bounds memory corruption via a specially crafted HTML page.

This is the second actively exploited zero-day vulnerability that Google has had to patch this year, the first being CVE-2025-2783.

Solution

Google recommends updating your browser to the following versions:

- Update to versions 137.0.7151.68 or 137.0.7151.69 for Windows or MacOS users.
- For Linux users, it is recommended to update to version 137.0.7151.68.

Affected Products

The vulnerability affects the following versions of Google Chrome:

- Versions earlier than137.0.7151.68.

References

- thehackernews.com
- nvd.nist.gov

Microsoft’s June security patches fix 67 vulnerabilities.

Date: June 10, 2025
CVE: CVE-2025-32711 and 66 more

Critical

Description

Microsoft has released patches fixing 67 vulnerabilities, including 2 critical ones. The most notable identified vulnerabilities are:

- CVE-2025-32711 (CVSS 9.3): Affects M365 Copilot and could allow an attacker to propagate information across a network via AI command injection.
- CVE-2025-47966 (CVSS 9.8): Allows privilege escalation by exposing classified information to a non-privileged user.

Additionally, some high-severity vulnerabilities include:

- CVE-2025-47167 (CVSS 8.4): A type confusion vulnerability in Microsoft Office enabling remote code execution.
- CVE-2025-47957 (CVSS 8.4): A use-after-free vulnerability in Microsoft Word that could allow remote code execution.

Affected Products

The vulnerabilities affect numerous Microsoft products. The full list of affected products can be found at the following link::

- msrc.microsoft.com

Solution

Microsoft recommends applying the released patch to remediate the vulnerabilities mentioned therein.

References

- msrc.microsoft.com
- thehackernews.com

Patch for the remote code execution vulnerability in WebDAV servers

Date: June 10, 2025
CVE: CVE-2025-33053

High

Description

The patch for this vulnerability, which affects servers running WebDAV on Microsoft IIS, Apache, and Nginx, was released on June 10, 2025, during Microsoft's Patch Tuesday.

The vulnerability was being exploited by the Stealth Falcon group. This update fixes an issue with path and filename validation that allowed remote attackers to execute malicious code on the server by manipulating the WebDAV protocol.

With this patch, the insufficient validation enabling exploitation is corrected, improving server security. Additionally, Apache and Nginx have released their own updates to address this vulnerability.

Affected Products

The affected versions include the following:

- Microsoft IIS versions prior to the patch released on June 10, 2025.
- Apache HTTP Server versions from 2.4.0 up to, but not including, version 2.4.57.
- Versiones de Nginx versions prior to the June 2025 update.

Solution

It is recommended to install the official patches released by Microsoft, Apache, and Nginx to fix the vulnerability. Additionally, disabling WebDAV where it is not necessary and monitoring access logs to detect potential attack attempts are advised.

References

- incibe.es
- microsoft.com

Events

RAISE Summit 2025
8 - 9 July

RAISE Summit 2025 will be held on July 8 and 9, 2025, at the Carrousel du Louvre in Paris. The event will bring together technology leaders to share practical cases of AI and Generative AI implementation, featuring a hackathon with over 300 participants focused on real-world solutions. It will include more than 150 investors driving disruptive innovations in AI.

Link

Data Center Asia 2025
15 - 17 July

Data Center Asia 2025 will take place from July 15 to 17, 2025, at AsiaWorld-Expo in Hong Kong, China. As a key event for digital infrastructure, cloud, AI, and cybersecurity in the Asia-Pacific region, it will bring together data center operators, IT specialists, security and sustainability experts, featuring over 100 conferences, panels, and solution booths. The event will focus on innovations in energy efficiency, facility design, AI, and strategies to protect against cyber threats.

Link

UserConf México 2025
16 – 17 July

UserConf Mexico 2025 will be held on July 16 and 17, 2025, at the Hilton Mexico City Reforma in Mexico City. The event will bring together IT leaders and professionals to explore the latest trends in IT management and cybersecurity, featuring hands-on workshops and technical sessions. There will be expert presentations and extensive networking opportunities.

Link

Resources

➢ Handbook for Cyber Stress Tests

The Handbook for Cyber Stress Tests published by ENISA provides a practical guide for national and sectoral authorities to assess the cyber resilience of critical infrastructures under the NIS2 directive. It defines cyber stress tests as targeted evaluations aimed at measuring the ability to withstand and recover from severe incidents, using realistic scenarios and resilience metrics. The handbook presents a clear five-step methodology: scope and objectives, scenario design, execution, gap analysis, and follow-up.

Link

➢ Likely Exploited Vulnerabilities

Likely Exploited Vulnerabilities (LEV) is a metric proposed by NIST that estimates the probability that a vulnerability has already been exploited in practice. Unlike KEV (Known Exploited Vulnerabilities) lists, which record confirmed cases, LEV uses historical data to identify vulnerabilities with a real likelihood of having been exploited. The methodology combines EPSS (Exploit Prediction Scoring System) scores over time to calculate the cumulative probability of past exploitation, thereby improving prioritization in patch management.

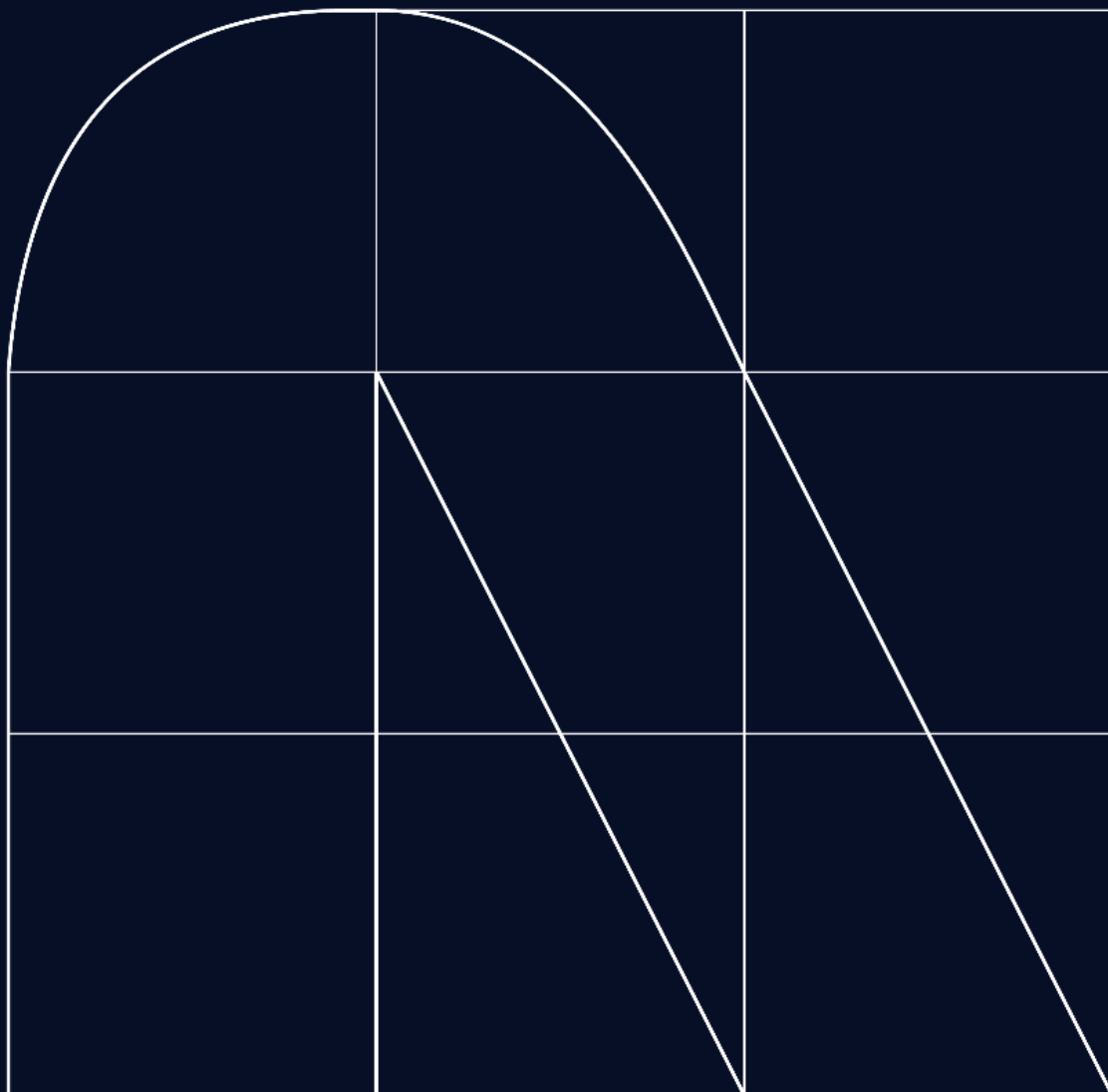
Link

➢ NIST Workshop Guide on Usable Cybersecurity and Privacy in Immersive Technologies

The NIST Virtual Workshop Guide on Usable Cybersecurity and Privacy in Immersive Technologies (IR 8557) addresses unique UX challenges related to security and privacy in virtual and augmented reality, exploring how immersive interfaces interact with biometric and behavioral data. It includes research presentations, an expert panel, and protocols to integrate usable protection in AR/VR environments.

Link

Subscribe to RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com