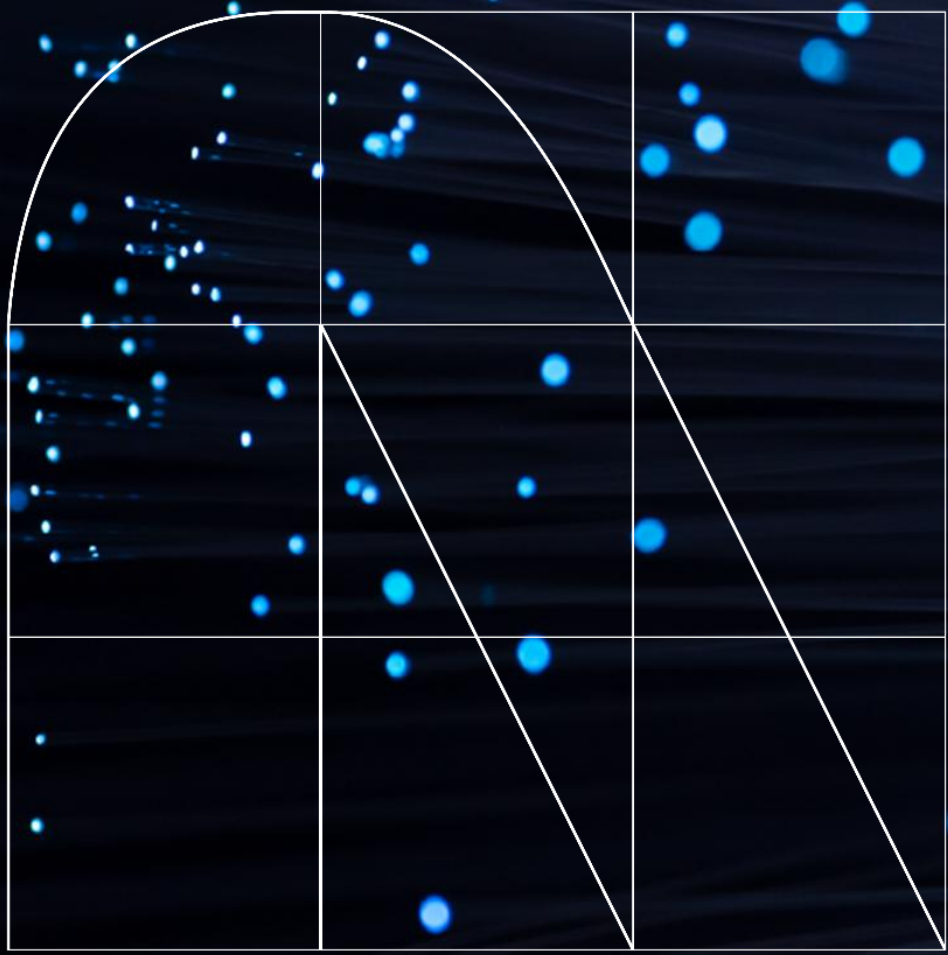
Issue 101 | April 2025

NTT DATA

Radar

The cybersecurity magazine



Cybersecurity: Protecting the future with innovation

By Andrea Isabel Muñoz Parreño

Currently, some of the challenges organizations face are the constant change and evolution of technology, as well as the behavior of consumers and clients. This requires them to innovate continuously in order to stay ahead and remain competitive when offering products and services. This business challenge is not indifferent to cybersecurity, as it too must keep up to date and be a core part of the business strategy in order to be a catalyst for growth, rather than an obstacle to it.

New trends such as the use of Artificial Intelligence, cloud adoption, quantum computing, among others, are making protection challenges increasingly complex and require an innovative strategy with strong allies, agile technologies, and skilled personnel. The very use and trend of Artificial Intelligence opens new attack vectors and increases the speed at which an organization can be attacked.

The big question is: how can we stay up-to-date with the new trends? How can we define a strategy that covers the most important risks of an organization and is sustainable over time?

The answer to these big questions lies not only in the involvement of expert companies as part of CISOs' strategies, but also in the community, in the sharing of trends and innovations in cybersecurity forums that allow companies to work in alignment, share experiences and concerns, and bring new ideas.

The RSA Conference 2025 (RSAC), held in San Francisco since 1995, offers that opportunity to participate in a community, discuss new trends, and engage with expert cybersecurity professionals and CISOs from all over the world in one forum. Each year, RSA has a different theme, and this year it will be "Many Voices, One Community," which is fully aligned with the idea of sharing knowledge and innovative ideas that are aligned with new technologies.

From NTT Data, we will be present at RSA from April 28 to May 1, sharing with our clients, bringing new trends, and conducting innovative demos, such as:

- **Security Insights:** A security platform that provides operational insights across multiple security domains.
- **Data Resilience:** Based on a company's ability to respond to security incidents.
- **MXDR for Integrated Threat Management:** For advanced protection of incidents, such as SOC trends.
- **Consumer IAM:** Focusing on how to address identity management while ensuring regulatory compliance and user experience.
- **Zero Trust Application Access:** To explore how organizations can monitor, detect, and protect critical application traffic in real time.

I hope that both the content of this magazine and the demos we will be presenting are of interest to you.

Andrea Isabel Muñoz Parreño
Cybersecurity Manager

Privacy in AI: A relevant enabler actor that sometimes operates without the necessary controls.

Cyberchronicle by Jaime Tovar Prieto

It is no mystery that the use of AI has become a fundamental tool for supporting personal, work-related, and, in some cases, emotional tasks. In this cyberchronicle, I would like to discuss the use of AI in any of its forms and one of the cases of "abuse" that has occurred due to the use of this technology, which has evolved into security incidents related to data breaches, due to the partial absence of proper security controls.

To address this, an incident will be discussed that may not have been widely known in the tech world, but has had a significant impact on some companies, understanding that not all events always point to the root cause. Below, I will discuss the case at the heart of this cyberchronicle.

What happens in Las Vegas, stays in Las Vegas, or, adjusted for this scenario, what gets indexed in Bing, stays in Bing. This is how the story begins. For this chronicle, we have a main actor named Copilot and a supporting actor named Bing (who undoubtedly deserves an Oscar). All of this takes us to mid-2024, when the security company Lasso observes a LinkedIn post accusing OpenAI of exposing data from private GitHub repositories (a code repository platform). Given the attention-grabbing nature of this alert, Lasso sets to work searching for the reason behind such an assertion and the unusual behavior indicated in the post.

After efforts to search and consultations with ChatGPT (OpenAI's own artificial intelligence), no clear indications were found regarding this behavior. When attempting to directly access some of the repositories that were supposed to be public, it was not possible, as they were private at that moment, making access impossible without valid and current authentication and authorization.

As the recurring inquiries continued with ChatGPT, the firm asked questions about its own repositories, where ChatGPT kept providing inconclusive answers about its repositories, meaning they were uninformative and only offered general concepts about the organization and the types of technologies it might have. So, what is happening?

The answer came later, when the same questions or validations were made in Copilot (Microsoft's own artificial intelligence), where it was possible to obtain information about the structure of those repositories, such as folder names, nesting, file sizes, among others; but at the time of the query, they were private, curious.

The answer was neither more difficult nor simpler, depending on how you want to look at it. It was simply Bing being Bing; it had managed to index the content through its crawlers and had cached those repositories it had detected as public at some point in time, very similar to the Wayback Machine (the time machine of the internet, where it is possible to access the state of a public website at a specific point in time).

And if it was Bing, why does Copilot have it?

The above occurs because Copilot uses Bing as its search engine to perform searches, which is both valid and functional. Based on this, it was possible to obtain what is known as Zombie Data, which refers to data that is not continuously used or has little usage (something very similar to cold data) and is available.

With clarity about what had occurred, Lasso escalated the issue to Microsoft for them to take the appropriate actions, receiving an effective response to their request and having the necessary solutions applied by Microsoft. Additionally, Lasso notified other companies affected by this behavior.

Up to this point, nothing out of the ordinary but still not normal, it is important not to normalize such incidents, as information leakage is highly relevant and can lead to economic impact and brand damage, not to mention the leak of proprietary brand secrets, something similar to what happened to Kaspersky some time ago.

From my point of view, up to this point, the only ones to blame are the administrators, who left the repositories exposed as public, which is a mistake, considering what they contained.

New year, new searches.

This takes us to mid-January 2025, more precisely, January 14th. At this point, Lasso decides to perform new searches on Bing for indexed repositories, receiving a 404 error message (HTTP error code indicating that a resource does not exist or has been moved) for several resources queried, which would be an expected response. Given the above, should we be at ease? The most obvious answer is yes.

In an attempt to investigate further whether it is possible to access these repositories, Copilot is used again, where the result was neither the same nor as expected, as it was possible to observe the repository structure and code fragments searched for, which could not be accessed through the search previously conducted on Bing.

So, why is it possible to access?

This could be understood to mean that the solution provided by Microsoft was not complete, as it is still possible to access private information that was once public through Copilot, since it could still access the cache that was disabled for user consumption in 2024, but possibly not for Copilot.

Something that, in my humble opinion, is very particular and striking. With the above, I am not suggesting that this should be used as a practice to bypass security controls, or anything of the sort, just that it is eye-catching to someone who requires special information that is not currently available.

For more information, consult the Lasso blog URL (link), where you can find more technical details on how to perform these types of searches (educational purpose).

General conclusions

Information Disclosure: Information is a very valuable asset for any organization and should be treated as such. All information should be categorized, prioritized, and handled according to its level of confidentiality.

Presentation of AI Results: At this point, I believe that while it is true that AI is a "living" product, based on its evolution model, it is crucial to review a bit more about the ethical component and the privacy topic, addressing the case presented in this story. With this, I don't mean to say that the stance is not appropriate, just that it is wise to place a bit more emphasis, and it will most likely become part of its evolution.

Partial Blocking of AI in the Organization: Currently, there are solutions from vendors in the market that can perform DLP (Data Loss Prevention) functions for AI, which can prevent users from accessing AIs, uploading, or viewing sensitive information in the AIs, thereby reducing the possibility of data breaches.

Jaime Tovar Prieto
Cybersecurity Architect

Post-Quantum Cryptography

Article by César Huanayque Vilca

In today's digital age, where information is an invaluable asset, information security has become a fundamental pillar for individuals, businesses, and governments alike. In this sense, cryptography has become a cornerstone for protecting the confidentiality, integrity, and authenticity of data. Over the past few decades, cryptography has evolved significantly, adapting to the growing threats and security demands in various industry sectors.

Cryptography, with its sophisticated encryption techniques, has played a crucial role in protecting sensitive data and ensuring secure communications, using mathematical encryption algorithms to safeguard data and transactions. Its application is critical across all economic sectors, including government and defense.

However, the landscape of cybersecurity is constantly evolving, and the advent of quantum computing presents new challenges that require a reevaluation of existing security paradigms.

Quantum computing has the potential to transform multiple industries, although it faces significant technical challenges, such as the development of stable and reliable qubits. Additionally, with its ability to perform calculations that exceed the capabilities of classical computers, and as quantum computers evolve, they could potentially undermine the effectiveness of many widely used cryptographic algorithms. This potential disruption calls for thorough research into new cryptanalysis strategies to assess the robustness of cryptographic systems against the capabilities of quantum computing.

Widely used cryptographic algorithms, such as RSA, ECC, and Diffie-Hellman, rely on mathematical problems that are difficult to solve for classical computers, but could be vulnerable to attacks from quantum computers. This means that information encrypted with these algorithms could be decrypted by attackers with access to sufficiently advanced quantum technology.

The role of AI

AI is revolutionizing cryptanalysis, providing new tools to analyze, attack, and defend cryptographic systems.

- **Enhanced analysis:** AI automates and improves pattern analysis in encrypted data, optimizes brute-force attacks, and facilitates the reverse engineering of algorithms.
- **Exposed vulnerabilities:** AI models identify weaknesses in modern encryptions and enable more sophisticated side-channel attacks.
- **Adapting to AI:** AI is also used to decrypt AI-based cryptographic systems, creating a race between the development of encryptions and the tools to break them.

AI and Quantum Computing

The convergence of Artificial Intelligence (AI) and quantum computing is opening an unprecedented chapter in cryptanalysis. The ability of AI to learn, optimize, and recognize complex patterns becomes a crucial tool for deciphering information security in the quantum era.

AI optimizes specific quantum algorithms, such as Shor's algorithm, by determining optimal parameters and mitigating errors. In Grover's algorithm, AI guides key searching and analyzes patterns to reveal hidden information.

What vulnerabilities can be deduced from future quantum computing?

Quantum computing, with its disruptive potential, poses a significant risk to current cryptography.

Although still in development, the ability of quantum computers to break current cryptographic algorithms is a real threat that could have high-impact consequences.

Potential Impact

- **Loss of Confidentiality:** Sensitive information, such as financial data, medical records, and government secrets, could be exposed.
- **Loss of Integrity:** Data manipulation and digital signature forgery could undermine trust in digital systems.
- **Loss of Trust:** The impact on e-commerce, online communications, and other activities that rely on cryptography could be severe.

The likelihood of quantum computers breaking cryptographic algorithms increases over time. In the short term, the risk is low to medium, but in the long term, the probability becomes significant. These probabilities may change depending on the evolution of quantum computers.

What actions can be taken?

The imminent arrival of quantum computing represents an unprecedented threat to current cryptography. To safeguard information in the long term, the adoption of post-quantum cryptography (PQC) becomes imperative. However, this transition is not trivial and requires meticulous planning and execution.

The implementation of PQC is not a one-time event, but an ongoing process that requires constant planning, implementation, and monitoring.

The standardization of algorithms is crucial to ensure compatibility between systems and communications. It should be considered that, as of today, there are already candidate standards from NIST to establish a standard framework for PQC.

The adoption of post-quantum cryptography (PQC) requires a process that can be distributed as follows:

Inventory and Evaluation: Identify systems, assess vulnerabilities, and prioritize migration.

1. **Research and Selection:** Follow standardization, evaluate algorithms, and select the appropriate ones.
2. **Testing and Implementation:** Conduct tests, plan the migration, and implement it gradually.
3. **Monitoring and Adaptation:** Monitor performance and adapt to changes in quantum security.

César Huanayque Vilca
Cybersecurity Expert Architect

Identity and Access Management: Challenges and Innovative Solutions

Article by Alicia Lara Herrera

In today's corporate environment, identity and access management has become a central pillar of organizational security. With digital transformation and the growing trend of remote work, companies face significant challenges in protecting their resources and ensuring regulatory compliance. Below, we delve into the key aspects of this complex landscape.

Credential Security and Multi-Factor Authentication

User credentials are the first line of defense against unauthorized access. Traditionally, passwords have been the most common method of authentication. However, due to the ease with which they can be compromised, organizations are adopting multi-factor authentication (MFA) technologies. MFA requires multiple forms of verification, such as something the user knows (password), something the user has (a mobile device), and something the user is (fingerprint or facial recognition).

Advantages and challenges of MFA:

- **Advantages:** It significantly increases the difficulty for malicious actors to access systems, as they would need to compromise multiple authentication factors**.**
- **Challenges:** Implementing MFA may face resistance from users due to the perceived additional complexity. Additionally, there are accessibility issues in contexts where users cannot easily access secondary devices.

Privileged Identity Management (PIM)

Privileged Identity Management focuses on controlling and protecting access to accounts that have elevated permissions. These accounts are attractive targets for attackers due to their ability to access critical systems.

Importance and Strategies of PIM:

- **Importance:** Preventing privilege abuse is crucial to avoid the exposure of sensitive data and the disruption of critical operations.
- **Strategies:** Companies must implement strict access controls, regular audits, and continuous monitoring of activities to detect and respond to potential privilege abuse.

Zero Trust: A New Paradigm

The Zero Trust security model is based on the principle that no entity, internal or external, should be trusted by default. Every access must be verified, and every action monitored.

Zero Trust Implementation:

Continuous Verification: Requires continuous authentication and authorization for each access request.

- **Constant Monitoring:** Organizations must implement real-time monitoring tools to detect anomalous behaviors and respond quickly to potential threats.

Digital Identity Based on Blockchain

Blockchain offers an innovative approach to identity management, providing an immutable record of identities that is verifiable and secure.

Benefits and Limitations:

- **Benefits:** The decentralized nature of blockchain reduces the risk of data manipulation and provides clear traceability of identity transactions.
- **Limitations:** The lack of standardization and the need for specific infrastructure limit its widespread adoption.

Identity Management as a Service (IDaaS)

IDaaS offers a cloud-based solution for identity management, enabling easy implementation and administration through scalable and flexible platforms.

Critical Aspects of IDaaS:

- **Ease of Implementation:** It allows organizations to outsource identity management, reducing the internal burden on IT teams.
- **Associated Risks:** Dependence on external providers can pose security risks and integration issues with existing internal systems.

Biometric Authentication

Biometric authentication, which uses unique physical characteristics such as fingerprints and facial recognition, offers a higher level of security compared to traditional methods.

Advantages and Challenges:

- **Advantages:** Significantly reduces the risk of identity theft by relying on characteristics inherent to the individual.
- **Challenges:** Privacy concerns and the secure storage of biometric data must be addressed to ensure user trust.

Regulatory Compliance and Identity Protection

Regulations like GDPR and LGPD require strict management of personal data, imposing severe penalties for non-compliance.

Compliance Requirements:

- **Personal Data Management:** Organizations must implement data protection policies that ensure the privacy and security of personal information.
- **Audits and Reporting:** It is crucial to maintain detailed records of access and activities to demonstrate compliance and respond to regulatory audits.

Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) are powerful tools in detecting fraud and suspicious behavior.

Security Applications:

- **Pattern Analysis:** These technologies enable the analysis of large volumes of data to identify patterns and anomalies that could indicate threats.
- **Proactive Response:** By detecting unusual behavior, systems can trigger alerts and automated responses to mitigate risks before they materialize.

In summary, identity and access management in the modern corporate environment requires a multifaceted approach that incorporates advanced technologies and best practices. By addressing these challenges with innovative solutions, organizations can effectively protect their assets and ensure regulatory compliance, thereby safeguarding their continuity and reputation in an increasingly digital world.

Alicia Lara Herrera
Cybersecurity Expert Engineer

Some quantum challenges

Quantum Space by María Gutiérrez

From the Quantum team at NTTDATA, we want to contribute to the dissemination of knowledge about quantum technology. As part of our activities, we are preparing a course on this subject with the following objectives:

- **Understand the fundamentals of quantum computing:** Explain the basic principles, the differences with classical computing, and its historical evolution.
- **Familiarize with quantum tools and simulators**: Introduce quantum environments and platforms allowing experimentation with basic quantum circuits.
- **Explore quantum algorithms and their applications:** Present key algorithms like Shor and Grover, analyzing their impact on optimization and cryptography.
- **Identify challenges and opportunities in the quantum field:** Analyze technological challenges, current limitations, and future trends in the adoption and scalability of quantum computing.

Next, I will share with you some of the content of the course that will help us approach the fundamental principles of quantum technology and computing, which we will discuss in the upcoming issues of the RADAR magazine this year. To understand the potential of this technology, it is essential to know four fundamental principles:

- **Qubits:** These are the basic unit of quantum information and can represent both 0 and 1 simultaneously due to superposition.
- **Superposition:** A qubit can be in multiple states at the same time, which gives quantum computers their incredible ability to parallelize computations.

- **Entanglement:** Es un fenómeno donde dos o más qubits están correlacionados de tal forma que el estado de uno depende del otro, independientemente de la distancia que los separe.
- **Quantum Interference:** It refers to how quantum states can combine and cancel each other out, allowing computation to be directed toward the correct solutions in specific algorithms.

Despite the immense value of quantum technology in revolutionizing multiple industries, its development and adoption face various technological, architectural, and infrastructure challenges. The transition from classical computational models to a quantum paradigm is not trivial and requires overcoming fundamental barriers in hardware, software, and implementation models.

Where are the main challenges?

1. Quantum hardware:

Quantum hardware is one of the most critical aspects in the evolution of quantum computing. The main challenges include:

- **Scalability of qubits:**Currently, the number of qubits available in quantum hardware varies significantly across different technological approaches. While IBM and Google are working on superconductors, D-Wave has developed annealers with thousands of qubits, although with limitations in their applicability.
- **Coherence time:** Qubits lose their quantum state due to decoherence in very short periods of time. This limits the number of operations that can be performed before the information degrades.

2. Infrastructure and adoption:

The integration of quantum computing into the current technological ecosystem requires overcoming several challenges:

- **Limitations in qubit connectivity:** The connections between qubits are not perfect. In architectures like D-Wave's, qubits must be chained together to represent variables, which creates stability and precision issues.
- **Commercial scalability:** Quantum computing is still in a developmental stage. While some problems can be solved with NISQ (Noisy Intermediate-Scale Quantum) hardware, true quantum advantage will require error-correcting hardware, which is still far from being a reality.

Arquitecturas y Modelos computacionales

Quantum computing models also present significant challenges:

- **Noise and errors in execution:** The execution of quantum algorithms on real hardware introduces noise that can affect the accuracy of results. Error mitigation strategies, such as Zero Noise Extrapolation, are under development, but they have not yet been fully resolved.
- **Problem encoding and mapping:** Unlike classical computing, problems must be represented in terms of quantum gates and the limited connectivity of qubits. This adds an additional layer of complexity in the design of algorithms.

In the next issue, we will discuss the main problems that are already benefiting from the application of quantum technology.

Cybersecurity of Tomorrow: Innovations that protect us today

Trends by José Cárdenas Camacho

In the digital age, the speed at which cybersecurity threats evolve requires companies to adopt innovative solutions to protect their assets and maintain operational continuity. Recent statistics indicate that global spending on cybersecurity exceeded $150 billion in 2024, with projections for an annual growth of 12% in the coming years. This landscape drives the constant search for disruptive technologies that transform digital defense.

New Paradigms in Digital Protection

The traditional defense model is no longer sufficient in the face of the sophistication of current attacks. Renowned organizations have started adopting Zero Trust architectures, which assume that no entity, whether internal or external, is trusted by default. According to Gartner, it is estimated that 70% of companies will implement this approach by 2026, reflecting an irreversible trend toward continuous verification of identities and access.

Emerging Technologies and Applications in Cyberattack Defense

Artificial Intelligence and Machine Learning:

Predictive analytics based on artificial intelligence allows for the identification of anomalous patterns in real-time. Machine learning algorithms are being trained to detect unusual behaviors, reducing response times to critical incidents. IDC studies forecast an annual growth of 28% in investments directed towards these technologies, highlighting their impact on early threat detection.

Blockchain and Data Security

Blockchain technology provides immutable traceability, which is essential for ensuring the integrity of information.

In sensitive sectors such as finance and healthcare, its application has significantly reduced the risks of fraud and data alteration, establishing itself as a cornerstone in the validation of digital transactions.

Quantum Cryptography

With the imminent era of quantum computing, quantum cryptography emerges as a revolutionary solution to protect the confidentiality of information. This technique uses principles of quantum physics to generate encryption keys that are virtually unbreakable, providing a strong barrier against the processing power of future attackers.

Automation and Orchestration of Responses

The integration of automation and orchestration systems enables a coordinated response to incidents. These tools facilitate the containment and mitigation of attacks by isolating compromised systems and deploying security patches instantly, which can reduce reaction time to emerging threats by up to 50%.

Impact and Projections in the Sector

The convergence of these technologies not only enhances security but also redefines the market. The cybersecurity innovations sector is projected to exceed $300 billion by 2027, driven by the increasing demand for adaptive solutions in an ever-evolving threat environment. Investment in R&D, along with strategic partnerships between the private sector and government agencies, is accelerating the digital transformation of cybersecurity defense.

Conclusion

The future of cybersecurity is defined by the integration of solutions that combine artificial intelligence, blockchain, quantum cryptography, and automation. These innovations, far from being passing trends, represent the path towards resilient and adaptive digital environments. In a context of growing threats, investing in innovation is not only strategic but essential to ensure the comprehensive protection of organizations in the digital age.

José Cárdenas Camacho
Cybersecurity Analyst

Vulnerabilities

Critical vulnerability in VMware products

Date: March 04, 2025
CVE: CVE-2025-22224

CVSS: 9.3

CRITICAL

Description

The critical vulnerability CVE-2025-22224, affecting VMware products, has been identified and reported by Broadcom Inc. It is a TOCTOU (Time-of-Check Time-of-Use) type flaw that leads to an out-of-bounds write.

If successfully exploited, this vulnerability allows an attacker with administrative privileges on a virtual machine to execute code on the host, such as the VMX process.Additionally, another high-risk vulnerability (CVE-2025-22225) has been classified, directly related to the first. This allows arbitrary writes to the kernel, potentially leading to an escape from the protected environment within the VMX process.

Solution

VMware has released security updates to address these vulnerabilities. The patches are available on the manufacturer's official portal.

It is recommended to update the affected products to the latest version as soon as possible.

Affected products

This vulnerability affects the following VMware products:

- ESXi 7.0 and 8.0
- Fusion 13.x
- Workstation 17.x
- Cloud Foundation 4.5.x and 5.x
- Telco Cloud Platform: 5.x, 4.x, 3.x, and 2.x
- Telco Cloud Infrastructure: 3.x and 2.x

References

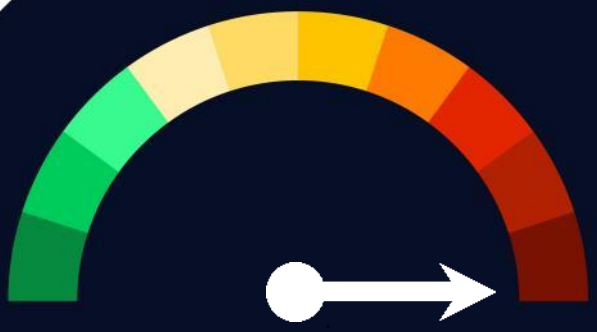
- cert.europa.eu
- broadcom.com

TLP:WHITE

Vulnerabilities

Critical Vulnerability in Kibana

Date: March 5, 2025
CVE: CVE-2025-25015



CVSS: 9.9

HIGH

Description

A critical vulnerability has been identified in Kibana (CVE-2025-25015), related to "Prototype Pollution," which allows an attacker to execute arbitrary code through the loading of manipulated files and specially crafted HTTP requests. It has been assigned a CVSS score of 9.9, making it a critical threat to affected systems.

This type of attack could allow the attacker to take control of the Kibana server, access sensitive data, and deploy additional payloads to further compromise the environment.

Solution

To mitigate the risks associated with this vulnerability, it is recommended to:

- Immediately update to Kibana version 8.17.3, where the issue has been fixed.

If an immediate update is not possible, a temporary mitigation can be applied by disabling the "Integration Assistant" functionality in the kibana.yml configuration file. To do this, the following line should be added:

```
xpack.integration_assistant.enabled: false
```

Affected products

The affected versions are as follows:

- V8.15.0 to V8.17.0: Any user with the "Viewer" role can exploit the vulnerability.
- V8.17.1 and V8.17.2: The vulnerability is only exploitable if the user has all of the following permissions: *fleet-all, integrations-all, actions:execute-advanced-connectors*.

References

- nvd.nist.gov
- discuss.elastic.co
- thehackernews.com

March Android Security Bulletin

Date: March 3, 2025
CVE: CVE-2024-43093 and 43 more

Critical

Description

The March 2025 Android Security Bulletin addresses a total of 44 vulnerabilities, including ten critical ones. The most severe of these is a vulnerability in the system component that, without requiring additional execution privileges, could lead to remote code execution.

Patches have also been released for two high-severity vulnerabilities that have been actively exploited:

- CVE-2024-43093: A local privilege escalation vulnerability, allowing unauthorized access to critical system directories.
- CVE-2024-50302: A vulnerability that, due to a privilege escalation flaw, could result in a kernel memory leak.

Affected products

The components affected by these vulnerabilities are:

- Framework
- Sistema
- Kernel
- Third-party components:
  - MediaTek
  - Qualcomm

Additionally, devices running Android 10 and later may also receive security updates.

Solution

Several security patches have been released in this bulletin, so it is recommended that all Android users update to the latest version to address the vulnerabilities.

References

- thehackernews.com
- android.com

Security Update for Microsoft Products

Date: March 11, 2025
CVE: CVE-2025-24983 and 56 more

Critical

Description

Microsoft has released security updates for 57 vulnerabilities, including 6 critical and 7 zero-days (six actively exploited and one publicly disclosed). Among the fixed vulnerabilities are privilege escalation, security feature bypass, remote code execution, information disclosure, denial of service, and spoofing.

Some of the most important zero-days include:

- CVE-2025-24983 (SYSTEM): Privilege escalation to SYSTEM exploiting a race condition.
- CVE-2025-24984 (NTFS): Allows reading memory fragments through malicious USBs.
- CVE-2025-24985 (FAT): Allows remote code execution via malicious VHD images.
- CVE-2025-24991 (NTFS): Information disclosure through manipulated VHDs.
- CVE-2025-24993 (NTFS): Remote code execution due to a buffer overflow in NTFS.
- CVE-2025-26633: Security bypass allowing the execution of malicious .msc files.

Affected products

Some of the affected products are:

- Windows 11: Versions 22H2 and 24H2.
- Windows 10: Versions 21H2 and 22H2.
- Windows Server 2022, 2019, 2016, 2012 R2.
- Microsoft Office 2016, 2019 and 2021.
- SharePoint 2013, 2016 and 2019.
- Visual Studio 2019 and 2022

Solution

Microsoft recommends immediate updating to the latest available version of each system and application.

References

- www.bleepingcomputer.com
- answers.microsoft.com

TLP:WHITE

Events

Forum InCyber Europe 2025
1 – 3 April

The Forum InCyber Europe 2025 will take place from April 1 to 3 at the Lille Grand Palais, France, establishing itself as one of the most significant events in the field of cybersecurity and digital trust in Europe. Under the theme "Beyond Zero Trust, trust for all," this edition will explore innovative strategies to strengthen security in an increasingly complex digital environment. The event will bring together experts, industry leaders, and key organizations in a combination of conferences, roundtables, and technical demonstrations, addressing topics such as risk management, digital sovereignty, and the fight against cybercrime.

Link

Black Hat Asia 2025
1 – 4 April

From April 1 to 4, 2025, the Marina Bay Sands Expo & Convention Centre in Singapore will be the epicenter of cybersecurity with Black Hat Asia 2025. This event will bring together global experts to discuss emerging threats, with a special focus on artificial intelligence, cybersecurity in financial services, and new vulnerabilities in mobile devices. The program will include advanced training, technical conferences, and presentations of innovative tools, as well as exclusive networking opportunities in its business lounge.

Link

Gartner Security & Risk Management Summit
7 – 8 April

The Gartner Security & Risk Management Summit 2025 will take place from April 7 to 8, 2025, at the Conrad Dubai, located in the United Arab Emirates. This event is designed for security and risk management leaders in the Middle East, offering a platform to discover the latest insights and solutions in cybersecurity. Attendees will have the opportunity to participate in sessions focused on key topics such as artificial intelligence in cybersecurity, cloud security, application security, and risk management and compliance.

Link

RSA Conference
28 April – 1 May

The RSA Conference 2025 will be held from April 28 to May 1, 2025, at the Moscone Center in San Francisco, California. Under the theme "Many times, one community," the event will bring together cybersecurity professionals to address critical topics such as artificial intelligence, cloud security, and risk management. The program will include keynote speeches, interactive sessions, and networking opportunities, providing a platform to share knowledge and explore innovative solutions in the field of digital security.

Link

Recursos

➢ ENISA NIS360

The ENISA NIS360 report, published by the European Union Agency for Cybersecurity (ENISA), assesses the maturity and criticality of the sectors covered by the NIS2 Directive, providing a detailed analysis of the cybersecurity state in key sectors such as energy, transport, finance, healthcare, and others. Based on data from national authorities, industry companies, and EU sources like Eurostat, this report is crucial in helping Member States identify gaps, prioritize resources, and strengthen cybersecurity resilience across the European Union.

Link

➢ NIST SP 800-226, Guidelines for evaluating differential privacy guarantees

The NIST Special Publication 800-226, issued by the National Institute of Standards and Technology (NIST), provides guidelines for evaluating differential privacy guarantees, a key mathematical technique for protecting personal information in data analysis. This document is essential in helping government organizations and businesses understand and effectively apply differential privacy, identifying critical factors and common risks in its implementation.

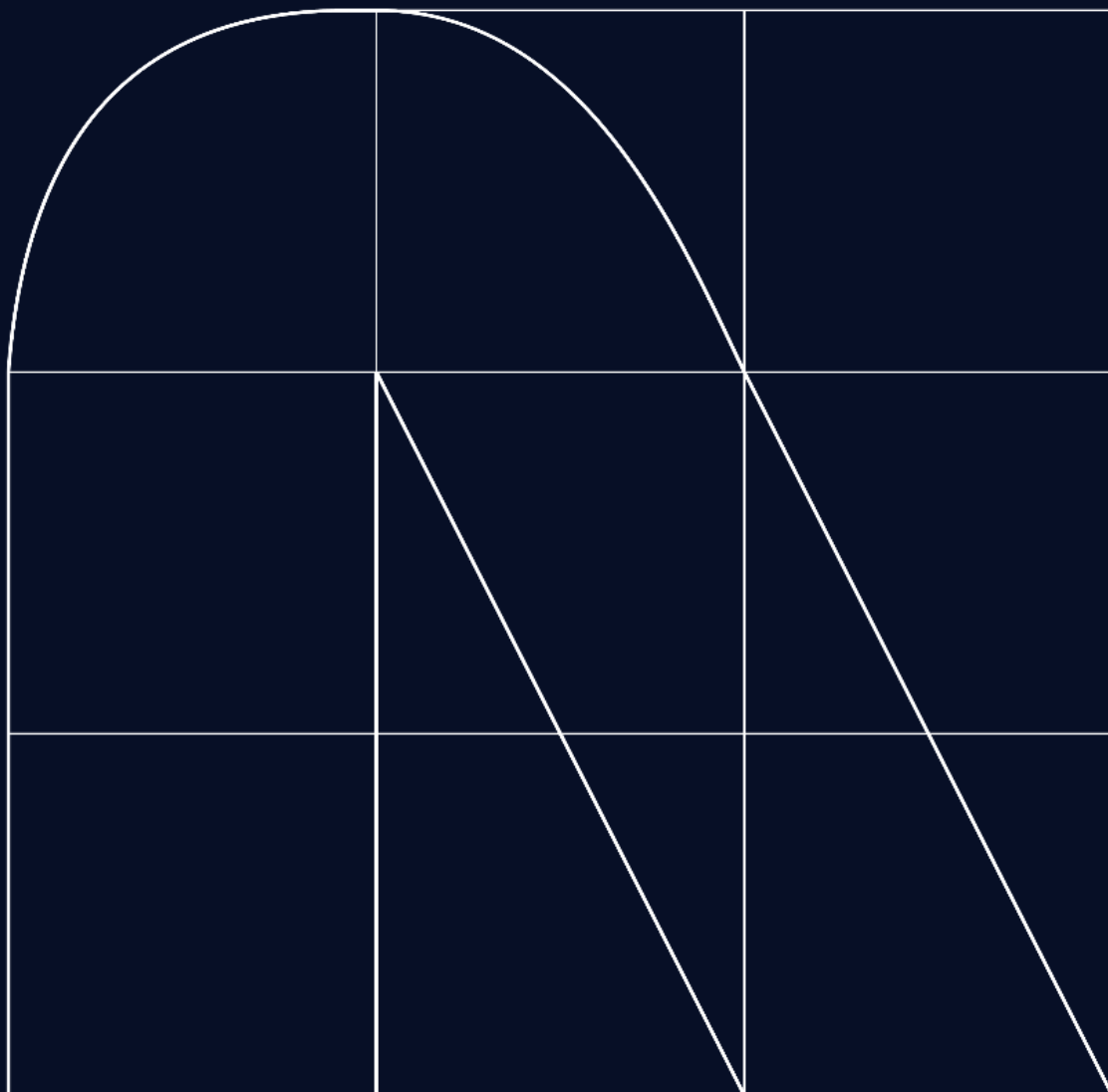
Link

➢ Entry into force of certain articles of Law 21.663

Recently, certain articles of Law 21.663, known as the Cybersecurity Framework Law in Chile, came into force. This legislation establishes a new governance model that promotes the implementation of cybersecurity standards in both the public and private sectors of the country. The law creates the National Cybersecurity Agency (ANCI) and defines specific obligations for Vital Importance Operators (VIO), including the implementation of information security management systems and operational continuity plans.

Link

Subscribe to RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com