Issue 95 | October 2024

NTT DATA

# Radar

## The cybersecurity magazine

# From cybersecurity to cyber-resilience

By María Pilar Torres Bruna

People who work in cybersecurity are observing how the frequency and sophistication of cyber-attacks are increasing, leading many organisations to accept that at some point they will become potential targets and that cyber attackers will succeed. For this reason, it is vital for companies to work not only on preventing these incidents but also on developing strategies to manage them effectively, with the aim of reducing their impact on operations and end customers.

Keeping critical processes of an organisation running during a cyber-attack is the primary objective of cyber-resilience. Achieving this goal involves implementing a series of processes, procedures, and technologies designed to sustain critical operations while the attack occurs—which can last several weeks—and continuing to provide service while the organisation recovers and returns to normalcy.

The terms cyber-resilience and cybersecurity are often confused, as, although they are different approaches, they complement each other. Cybersecurity focuses on protection and detection, meaning the main emphasis is before the attack; cyber-resilience prepares the organisation to face and recover from an attack by creating effective contingency plans and fostering an organisational culture that teaches employees how to act without certain usual systems or tools for their work.

Indeed, the preparation of staff is essential in any cyber-resilience plan. While cybersecurity training aims for employees to identify potential threats and adopt preventive behaviours, education in cyber-resilience focuses on how to react to an incident, including continuing work without the affected systems. How do I assist bank customers during an attack? How can I continue selling my products? How do I keep issuing boarding passes?

Organisations must be aware of their cyber-resilience posture, which should improve each year. In the face of increasingly sophisticated and common cyber-attacks, only a cyber-resilient company can mitigate economic losses, reduce the investment needed for recovery, and decrease costs related to penalties and litigation. Furthermore, it minimises harm to third parties, preserves its reputation, and maintains its competitive edge, thereby remaining prepared to lead in the future.

Given the importance of cyber-resilience for the future, we have decided to dedicate this month's RADAR to this theme.

**María Pilar Torres Bruna**
Cybersecurity Director

# Digital security under attack

Cyberchronicle by Yeiber Basilio Caso Ramirez

Recently, the world of cybersecurity has witnessed several significant incidents. From cyber attacks on major banks and e-commerce companies to critical vulnerabilities in railway systems and mobile devices, digital security remains a constant challenge. Here, we present a summary of the most notable news from the month.

In particular, JPMorgan Chase suffered a cyber attack that exploited a zero-day vulnerability, allowing attackers to divert large sums of money and compromise customer data, causing significant damage to the bank's reputation.

Meanwhile, Amazon experienced a massive data breach. Cybercriminals stole personal information and credit card data from millions of customers, later leaking it on the dark web. This resulted in numerous cases of identity theft and unauthorised transactions.

A group of researchers demonstrated how to exploit vulnerabilities in Renfe's railway system, allowing malicious actors to send commands to trains and potentially stop them. This discovery underscores the urgent need to strengthen security in critical infrastructures.

In the realm of mobile devices, a vulnerability has been discovered in the basebands of 5G mobile devices manufactured by Samsung, MediaTek, and Qualcomm. This flaw allowed attackers to spy on users without their knowledge. However, the manufacturers have implemented the necessary fixes to mitigate this threat. A zero-day vulnerability was also found in the Telegram messaging app for Android, dubbed 'EvilVideo', which allowed attackers to send malicious APK files disguised as videos, compromising users' devices.

One of the most alarming episodes involved the exploitation of zero-day vulnerabilities in "Versa Director," perpetrated by the Chinese group APT Volt Typhoon. This attack targeted the critical internet infrastructure in the United States, where it was discovered that numerous organisations had not implemented adequate security measures, leaving crucial management ports exposed.

This incident underscores the urgent need to improve cybersecurity practices, especially in infrastructures that support vital services.

At the same time, one of the largest data breaches in recent history was reported, affecting 3 billion people. This event highlighted the vulnerability of companies engaged in data aggregation, which, when compromised, expose the information of millions of users. Additionally, the multinational Toyota fell victim to a data breach in which 240 GB of employee and customer information was leaked, although the attack originated through a third-party supplier.

Furthermore, a ransomware attack affected 200 companies in the United States, including Kaseya. The systems were compromised by cybercriminals who demanded a ransom to unlock them, causing significant disruptions in the operations of the affected companies.

In Europe, Spain was not immune to this wave of cyber attacks. Several Spanish companies in the financial and energy sectors reported significant incidents, particularly ransomware attacks that temporarily paralysed their operations.

Attackers used advanced variants of ransomware that encrypted critical data and demanded payments in cryptocurrencies, making it difficult to recover the affected systems.

In Latin America, Chile experienced a significant attack on its energy infrastructure. A ransomware group, which recently rebranded as APT INC, launched an attack that compromised VMware ESXi servers, widely used in critical systems. This group is known for its sophistication and for employing advanced encryption tools, complicating victims' responses.

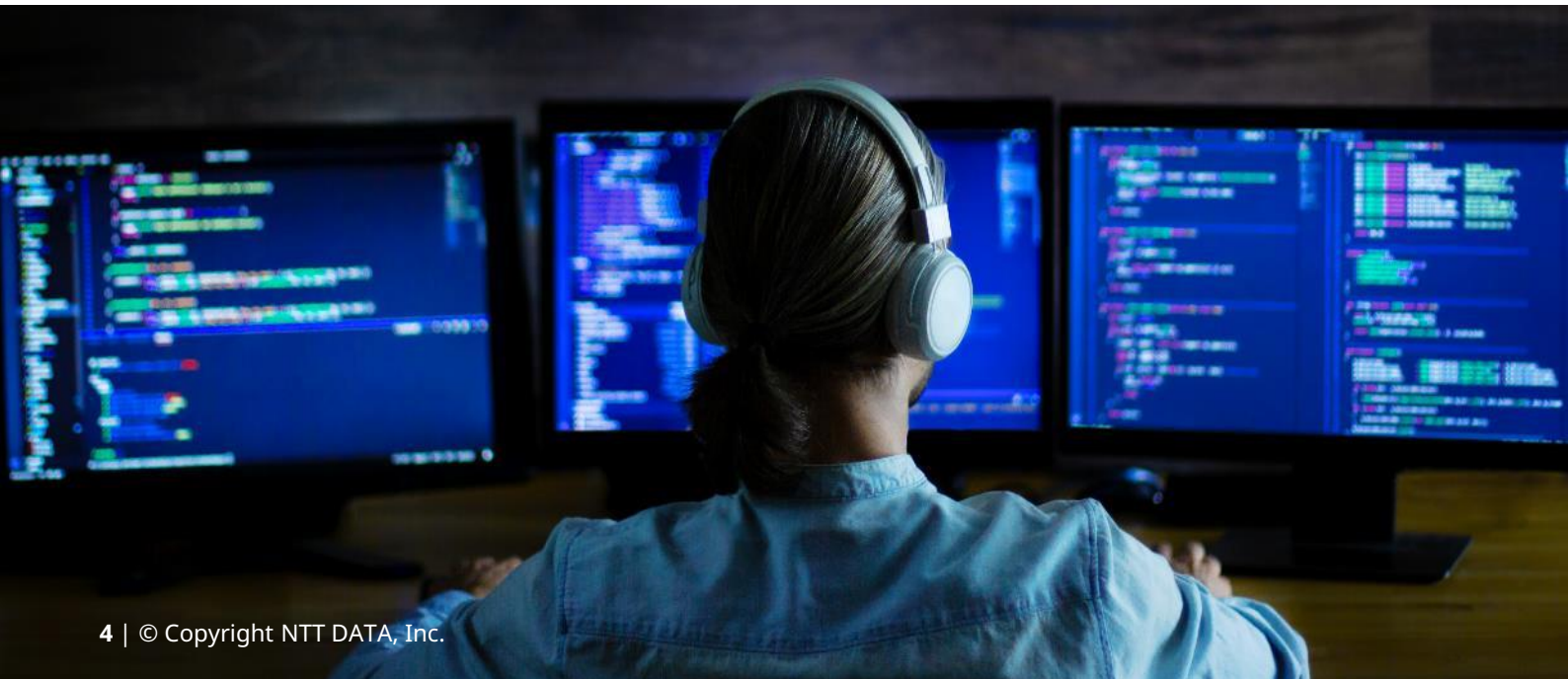
 

In the realm of critical infrastructures, SeaTac airport and several maritime ports in Seattle suffered operational disruptions due to cyber attacks that forced a return to manual processes, severely impacting logistics and transportation. These attacks highlight the vulnerability of sectors that rely on interconnected digital systems.

Globally, there has been a notable increase in vulnerabilities related to privilege escalation. In a recent security report, 36 vulnerabilities of this type were identified, highlighting the growing trend of attackers exploiting these flaws to gain full control over compromised systems. These incidents have underscored the critical importance of keeping systems updated and applying security patches as quickly as possible.

In conclusion, this period has been marked by a series of cyber attacks that not only affect individual companies but also pose risks to critical infrastructures and the national security of several countries. The evolution of these threats demands a coordinated and effective response at both governmental and corporate levels to mitigate risks and protect the most valuable information and assets of global society.

**Yeiber Basilio Caso Ramirez**
Technical Manager



# Journey to cyber-resilience

By Alberto Faus Avila

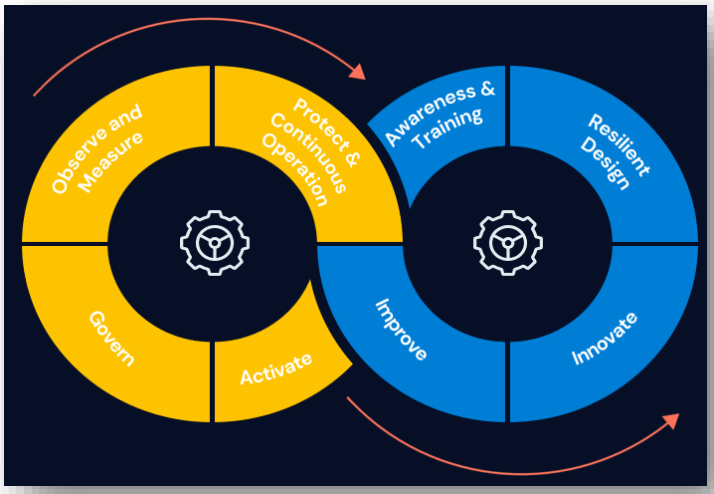
If anything has taught us about the CrowdStrike outage in July, it is that we are much more vulnerable than we thought to incidents related to technology. We must be better prepared for these eventualities so that they do not impact us, meaning we need to be more cyber-resilient.

Cyber-resilience is about that; it is not a Disaster Recovery Plan, nor cybersecurity, and it is certainly not a product that you purchase which magically makes your organisation cyber-resilient.

It is the ability of an organisation to continue delivering expected results despite any adverse technology-related situations. It prepares us to respond, recover, and adapt to these events, ensuring the protection and recovery of our information systems through planning and preparation before they occur.

For this reason, it is important to introduce cyber-resilience into our organisations, and to achieve this, we must have a clear roadmap that should include the following steps:

- **Current Maturity Level**: The path to cyber-resilience begins by understanding where we stand in all areas of IT, not just in cybersecurity. In this way, we will analyse the following elements: IT governance, security processes, networks and systems, the level of training and awareness of our staff, the preparedness of our organisation's leaders regarding cyber-resilience, identification of critical assets within our company, documentation, risk management, continuous operational capability, observability, etc. All these elements and more should be under our scrutiny, and we must conduct an assessment on all of them to determine our starting point in order to understand the path we need to take to reach our goal.
- **Strategy**: Once we have the results of this assessment, a collective and long-term strategy is essential for success. A holistic view of cyber-resilience and strong organisational commitment is critical, and not just from the organisation alone. Today, collaboration with third parties is vital in our ecosystems, and we must take this into account. We need to take a step forward and move from the short-term benefits of individual security to the long-term vision of Collective Resilience, which requires a strategic and step-by-step approach. We must clearly define and map our IT ecosystems and understand their dependencies. Understanding this and the associated risks will provide us with a clear vision of the objectives we need to prioritise.
- **Getting Started**: Once we know our current state, our objectives, and our strategy, we must begin to mature our weakest points through projects that address the most critical areas in any of the analysed domains. It is important to understand that defining, developing, and improving our IT ecosystem to enhance our cyber-resilience is not a short-term strategy, as it requires strong leadership with a long-term vision and the ability to foster collaboration among individuals and groups within our organisation.
- **Continuous Cycle**: cyber-resilience is not a time-bound activity; it is a cultural change and a series of cyclical activities that we must not forget, requiring constant review, improvement, evolution, and innovation.




Our organisations must migrate from cybersecurity to cyber-resilience as the next step in the evolution toward achieving zero impact in the upcoming challenges that the technological world may present in the future. Nowadays, the question is not if it will happen, but rather when.

**Alberto Faus Avila**
Manager

# Regulatory cyber-resilience: a key pillar for digital security

By Melanie Brenis Valencia

Nowadays, the rapid technological advancement has transformed the way organisations operate, as they increasingly rely on digital processes. However, it is undeniable that this transformation has also led to a significant increase in the cyber risks to which they are exposed. And that is where a key concept comes into play: cyber-resilience.

Ensuring cyber-resilience not only means that organisations are prepared to prevent cyberattacks, but primarily that they have the capacity to recover quickly from them and maintain operational continuity.

To achieve this, regulations play an essential role, as they allow for the establishment of common standards that strengthen the security of organisations. Without clear regulations, cyber-resilience may be compromised, affecting both businesses and end clients.

Indeed, the European Union (EU) has been a pioneer in developing regulatory frameworks for cyber-resilience, with some of the most notable being Regulation EU 2022/2554, the Digital Resilience Operational Act (also known as "DORA"), and the proposed cyber-resilience Act (also known as "CRA"). Both frameworks aim to establish clear guidelines to enhance the cyber-resilience capacity of organisations, each focused on different areas.

- **Regulation EU 2022/2254, Digital Resilience Operational Act (DORA):**

The Digital Operational Resilience Act (DORA) was officially published in the Official Journal of the EU on 27 December 2022 and will come into force on 17 January 2025. This regulation is specifically aimed at entities within the financial sector, including banks, insurers, payment service providers, and other key players in the financial ecosystem. Its main goal is to ensure that such entities can withstand, recover, and continue to operate securely in the face of any type of cyber incident and/or cyberattack.

The key provisions established by DORA for financial entities revolve around:

✓ **ICT Risk Management**: Organisations must have a governing body in charge of ICT risk management and implement robust frameworks to properly and effectively protect their physical infrastructures and ensure digital resilience.

- ✓ **Digital Operational Resilience Testing:** Organisations must conduct regular tests to assess their preparedness and ensure the identification of shortcomings, deficiencies, or gaps.

- ✓ **ICT-related Incidents:** Organisations are required to monitor and record incidents they have faced and report any serious ICT-related incidents to the relevant authorities.

- ✓ **Third-party ICT Risk Management:** Organisations must ensure that their ICT service providers also comply with the established legal and technical security standards.

- ✓ **Information Sharing Agreements:** Organisations may establish agreements to exchange cyber threat intelligence with peers, strategic partners, etc.

- **Cyber-Resilience Act Project**

The Cyber-Resilience Act (CRA) is a regulatory project by the European Union, presented in September 2022. Although it has not yet been officially adopted, it is expected to come into force by the end of 2024. Unlike DORA, the CRA has a broader scope, focusing on the security of digital products, such as smart devices, software, and applications, aiming to reduce vulnerabilities from their design.

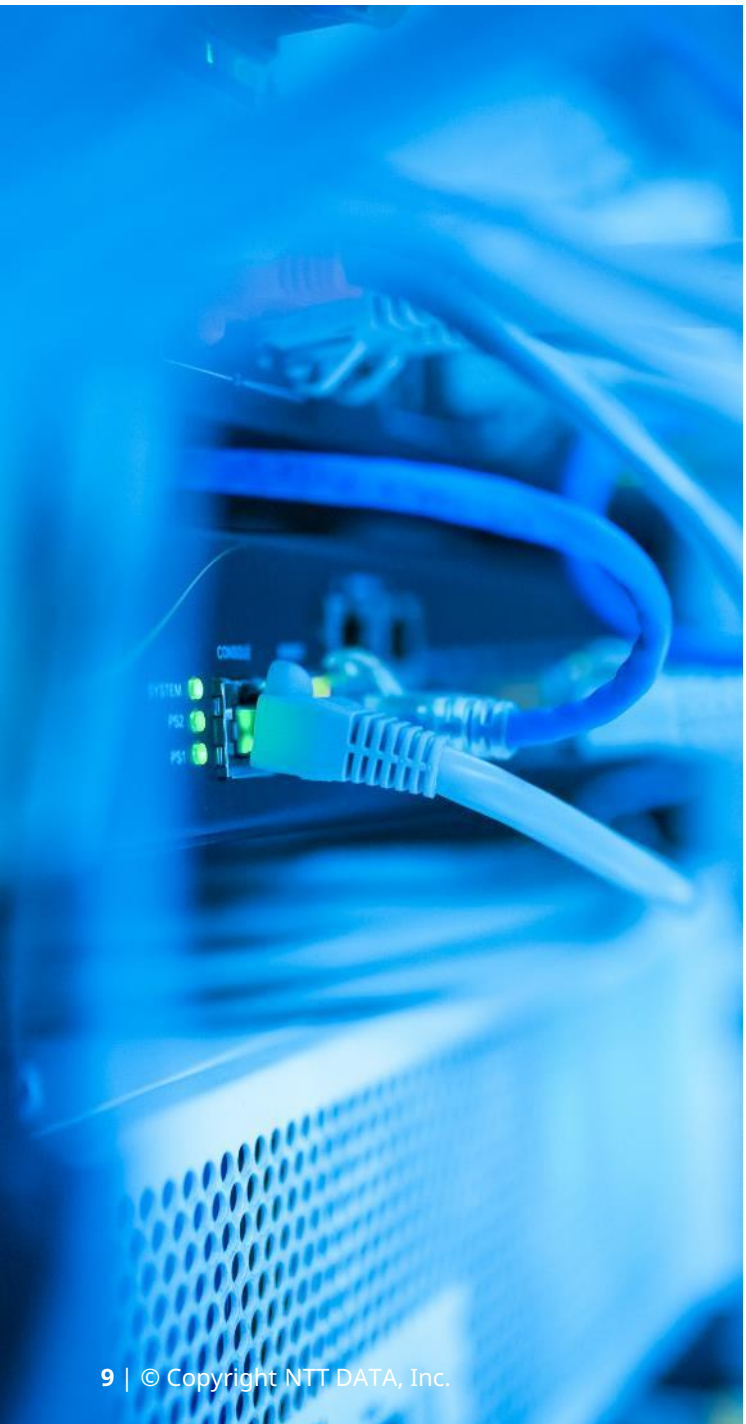
The main provisions that the CRA establishes include:

- ✓ **Security by Design**: Organisations must ensure that their products come with secure default configurations, reducing exploitable vulnerabilities.

- ✓ **Security updates**: Organisations must ensure that vulnerabilities in their products can be addressed through security updates, including automated updates.
- ✓ **Personal data**: Organisations must ensure that their products protect the confidentiality and integrity of personal data processed, for example, through encryption of data at rest or in transit.
- ✓ **Availability of functions**: Organisations must ensure that their products protect the availability of essential functions, including resilience against denial-of-service attacks and the mitigation of their effects.

As we can see, regulatory cyber-resilience represents a crucial step towards creating a more secure and resilient digital environment against cyber threats. Regulations like DORA and the proposed CRA not only set clear obligations for key sectors but also signal a shift towards greater responsibility in digital security.

As organisations prepare to comply with these frameworks, the focus on cyber-resilience becomes a vital element for economic and operational stability in an increasingly interconnected world.



**Melanie Brenis Valencia**
Cybersecurity Senior Consultant

# Auto Coding Agent

Trends by Alberto Faus Avila

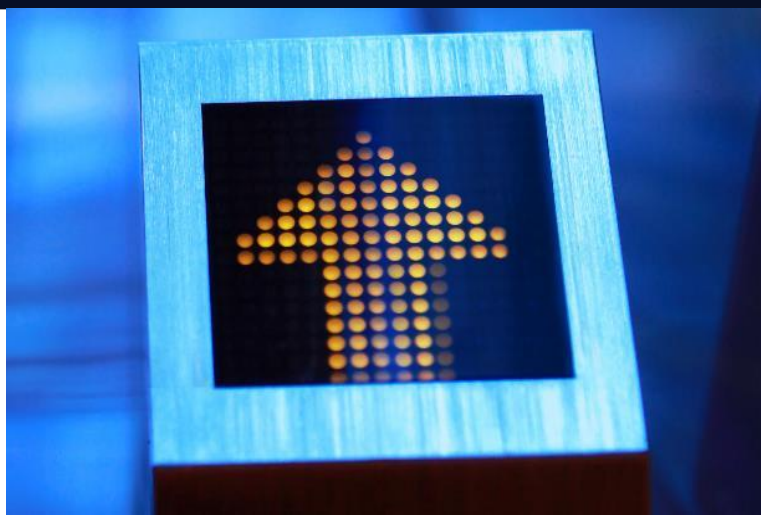
In development teams, it is estimated that at least a quarter of the team spends their day improving code. This means that a significant portion of their effort is focused on fixing issues rather than adding value to the business.

When an incident occurs, a significant amount of time is spent recovering applications, even though, in many cases, the necessary actions are well-known. The only requirement is a timely evaluation and execution of the next steps.

It is also worth noting that substantial efforts are made to review and improve applications as part of continuous improvement. However, this often leads to a loss of focus on log review and error verification.

NTT DATA's solution to this issue is the Auto Coding Agent, an intelligent system responsible for auto-remediation and auto-evolution. This solution aims to address the challenges by automatically handling known issues and ensuring continuous improvements without manual intervention, allowing development teams to focus on adding business value instead of merely fixing code:

- The agent monitors application logs in real-time. Based on its knowledge, it determines whether an issue is an error or a warning, whether it's related to the platform or the application itself.
- In the case of platform-related incidents, the agent analyzes previous successful solutions and makes the best decision by executing the commands needed to restore the platform to its optimal state.
- In the initial phase, the agent can analyze incidents and introduce the optimal code, which can then be reviewed by a technical lead before going into production. In the near future, human intervention will no longer be necessary unless desired, transitioning into a fully automated phase.



The Auto Coding Agent represents the future of application support, serving as a significant lever for operational efficiency and enhancing the quality of our application development services.

**Alberto Faus Avila**
Manager

# Vulnerabilities

## Critical vulnerability in FileCatalyst Workflow

**Date:** August 27, 2024
**CVE:** CVE-2024-6633

**CVSS: 9.8**

**CRITICAL**

## Description

The critical vulnerability CVE-2024-6633 in Fortra's FileCatalyst Workflow software originates from the publication of default credentials for the HSQL configuration database (HSQLDB) in a vendor article.

The cybersecurity solutions company Fortra notes that HSQLDB is deprecated and not intended for production use, although it remains included in FileCatalyst Workflow.

The vulnerability would allow an attacker with network access and port scanning capability to gain remote access to the database using the default credentials, potentially manipulating and/or exfiltrating data, as well as creating administrative users.

## Solution

Fortra has addressed the vulnerability by restricting access to the HSQLDB database solely to localhost.

The company recommends not using the included HSQL database and emphasises that the vulnerability can only be exploited if the attacker has network access, performs port scanning, and if the HSQLDB port is exposed to the Internet.

Patches are included starting from version 5.1.7 build 156 of FileCatalyst Workflow, which also resolves a high-severity SQL injection vulnerability identified as CVE-2024-6632.

## Affected products

The vulnerability affects the following versions:

- Versions of FileCatalyst Workflow from 5.0.4 to 5.1.6.139.

## References

- fortra.com
- cvedetails.com
- securityweek.com
- unaaldia.hispasec.com

TLP:WHITE

# Vulnerabilities

## Multiple vulnerabilities in Cisco products

**Date:** September 4, 2024
**CVE:** CVE-2024-20439 and 5 more

**CVSS: 9.8**

**CRITICAL**

## Description

Cisco has revealed 6 vulnerabilities, including 2 critical, 1 high, and 3 of medium severity. The critical vulnerabilities are:

- CVE-2024-20439: An unauthenticated remote attacker can exploit an undocumented static administrative credential to gain full system access with administrator privileges.
- CVE-2024-20440: Excessive detail in debug log files allows an attacker, via a malicious HTTP request, to access sensitive information such as API credentials.

## Solution

To address these vulnerabilities, Cisco has released several security patches, which are included in a single software version.

Affected users are advised to update to the following version as soon as possible:

Cisco Smart License Utility: Update to version 2.3.0.

## Affected products

The critical vulnerabilities previously described affect the following versions of Cisco Smart License Utility:

- Cisco Smart License Utility version 2.0.0
- Cisco Smart License Utility version 2.1.0
- Cisco Smart License Utility version 2.2.0

## References

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



TLP:WHITE

# Security updates for vulnerabilities in Veeam products

**Date:** September 4, 2024
**CVE:** CVE-2024-40711 and 17 more

**Critical**

## Description

Veeam has released a new bulletin with security updates addressing 18 critical and high-severity vulnerabilities in its products Veeam Backup & Replication, Service Provider Console, and One.

Among the vulnerabilities fixed is the critical vulnerability CVE-2024-4071 (with a score of 9.8). This vulnerability affects Veeam Backup & Replication (VBR) and allows unauthenticated remote code execution (RCE).

Although the vendor has not disclosed many details, the vulnerability could allow an attacker to gain full control of the system through the deserialisation of .NET Remoting

## Affected products

The vulnerabilities published in the bulletin affect the following products:

- Veeam Backup & Replication 12.1.2.172 and all 12.x versions.
- Veeam Agent for Linux 6.1.2.1781 and all 6.x versions.
- Veeam ONE 12.1.0.3208 and all 12.x versions.
- Veeam Service Provider Console 8.0.0.19552 and all 8.x versions.
- Veeam Backup for Nutanix AHV Plug-In 12.5.1.8 and all 12.x versions.
- Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization Plug-In 12.4.1.45 and all 12.x versions.

## Solution

It is recommended to apply the updates released by the vendor in their security bulletin.

## References

- bleepingcomputer.com
- veeam.com
- watchtowr.com

TLP:WHITE

# Critical security update for Ivanti Endpoint Manager

**Fecha:** September 10, 2024
**CVE:** CVE-2024-29847 and 9 more

**Critical**

## Description

Ivanti has released several software updates to address multiple critical vulnerabilities affecting Endpoint Manager (EPM).

The main vulnerability identified, with a score of 10.0, is CVE-2024-29847, a deserialisation vulnerability that allows an unauthenticated remote attacker to execute code.

An additional 9 critical vulnerabilities fixed with this update involve unspecified SQL injection flaws, which could allow an authenticated attacker with administrative privileges to execute code remotely.

Ivanti has confirmed that these vulnerabilities were discovered through internal scanning, manual exploitation, and testing. Furthermore, the company has stated that, as of the release of this security update, no active exploitation of these vulnerabilities has been detected, nor are there any known indicators of compromise.

## Affected products

The affected EPM versions are:

- Endpoint Manager: version 2024. It should be updated to version 2024 SU1.
- Endpoint Manager: version 2022 SU5 and earlier. It should be updated to version 2024 SU6.

## Solution

Ivanti recommends applying the patches published in their security update, depending on the affected version of Endpoint Manager in use.

## References

- bleepingcomputer.com
- thehackernews.com
- ivanti.com

# Events

### Cybersecurity & Cloud Expo (1-2 October)

The Cyber Security & Cloud Expo is a major event that will be held in Amsterdam from October 1 to 2, 2024. It will bring together more than 7,000 attendees and 150 industry experts to discuss crucial topics such as cloud security, threat detection, Zero Trust, hybrid cloud adoption, and DevSecOps integration. It is a key opportunity to learn about the latest innovations and strategies in cybersecurity and cloud technology.
**Link**

### PCI SSC Europe Community Meeting (8-10 October)

The PCI Security Standards Council (PCI SSC) Europe Community Meeting 2024 will be held in Barcelona from October 8 to 10. This event is crucial for data security and compliance professionals, as it brings together PCI DSS experts to discuss updates, best practices, and the evolution of security standards in the payments industry.
**Link**

### World Summit AI (9-10 October)

The World Summit AI 2024 is a global event that brings together artificial intelligence experts, business leaders, and technologists in Amsterdam to explore the latest innovations in AI. This event covers topics such as ethics in AI, artificial intelligence in the cloud, and cybersecurity related to AI systems. It is a key platform to learn about advances, make connections and discuss the future of artificial intelligence globally.
**Link**

### It-sa Expo & Congress (22-24 October)

The it-sa Expo & Congress 2024 is Europe's leading trade fair for IT security, which will take place from 22 to 24 October in Nuremberg. This event brings together experts and decision-makers from various sectors to discuss the latest trends in cybersecurity, including critical infrastructure protection, cloud security, and threat defense. It is an essential platform for exploring security innovations and establishing key contacts in the industry.
**Link**

### ISACA 2024 Europe Conference (23-25 October)

The ISACA 2024 Europe Conference is a prominent event that will be held in Dublin from 23 to 25 October 2024. This event includes a wide variety of educational sessions, interactive workshops, and panel discussions. Topics range from risk management to cybersecurity and governance, offering professionals an opportunity to delve deeper into current challenges and emerging trends in the technology industry.
**Link**

# Resources

### Addictive patterns in the processing of personal data

The AEPD (Spanish Data Protection Agency) published a document titled “Addictive Patterns in the Processing of Personal Data: Implications for Data Protection.” This bibliographic resource analyses how certain digital designs and strategies can manipulate user behaviour, encouraging excessive or addictive use of applications and services. It also emphasises the importance of ensuring that companies adopt ethical practices in interface design and personal data management, and it proposes guidelines to avoid exploiting users' psychological vulnerabilities.
**Link**

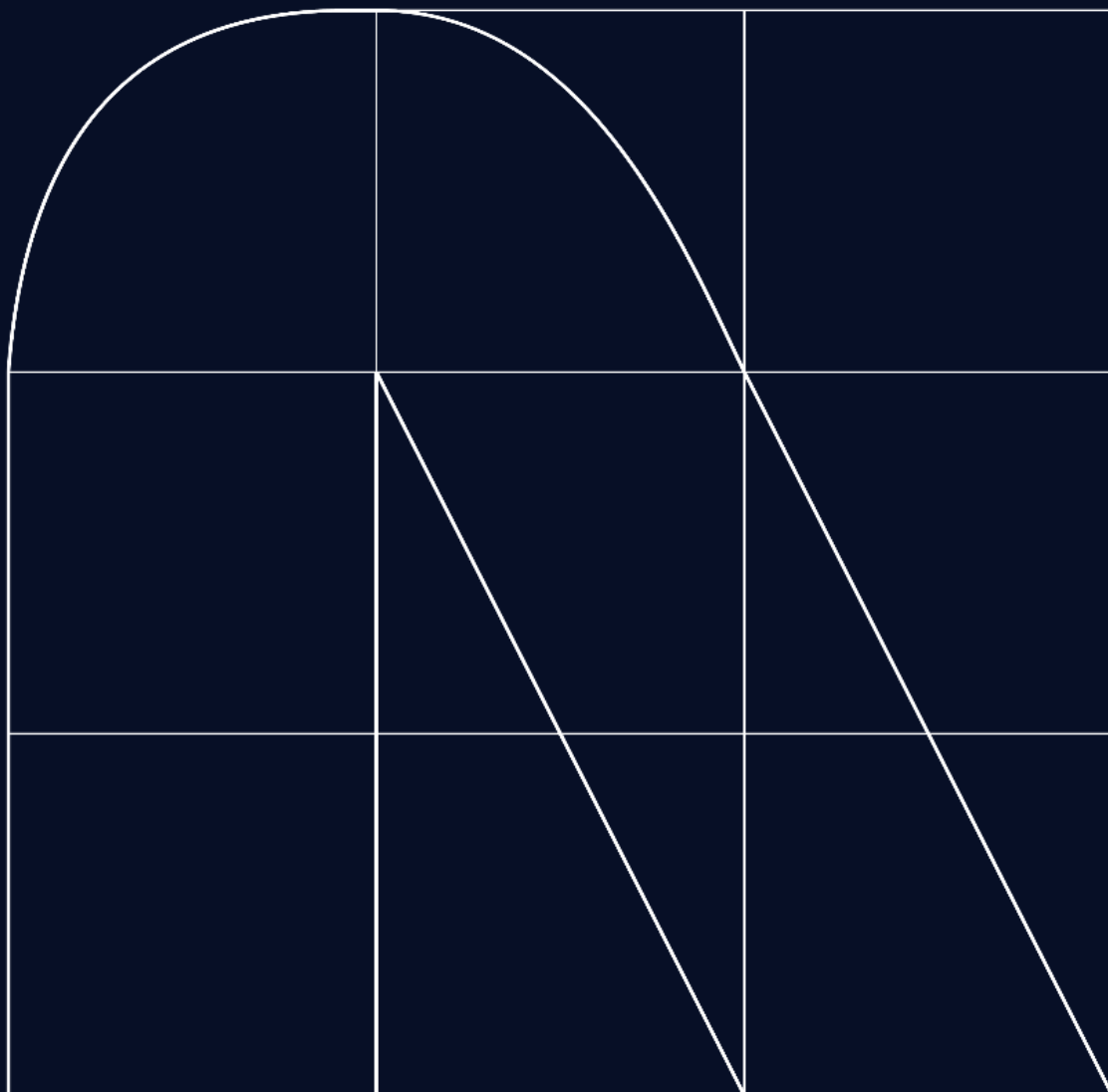
### Second set of policies under the Digital Operational Resilience Regulation

The European Supervisory Authorities (ESAs) have published the second set of policies under the Digital Operational Resilience Regulation (also known as "DORA"). This includes guidelines and technical specifications for the implementation of DORA, addressing key aspects such as technology risk management, supervision of third-party providers, and incident reporting requirements, in order to strengthen the stability of the European financial system against digital threats. Currently, the second set of policies is under review by the European Commission, with the final version expected to be issued in the coming months; however, they serve as an excellent bibliographic resource for review in the meantime.
**Link**

### Post-quantum encryption standards

NIST has finalised the first three post-quantum encryption standards, designed to protect electronic information against future threats from quantum computers. These standards, developed over eight years, include algorithms for general encryption and digital signatures, ensuring security in a post-quantum world. NIST urges immediate adoption of these standards to prepare for potential cyberattacks based on quantum technology.
**Link**

**Subscribe to RADAR**



**Powered by the cybersecurity NTT DATA team**

es.nttdata.com