NUMBER 75 | FEBRUARY 2023

NTT DATA
Trusted Global Innovator

# Radar

## Cybersecurity magazine

# PRIVACY RISK MANAGEMENT. A CENTRAL ELEMENT FOR TRUST IN THE ORGANIZATION

International Personal Data Protection Day is celebrated internationally on 28 January, in connection with Convention 108, which protects individuals with regard to the automatic processing of personal data. This is not only relevant because of the importance of the use of personal data in various sectors, but also because of recent international news about security breaches in which customer or employee information may be involved and, therefore, the reputational damage faced by organisations.

A constant challenge for organisations is to strike a balance between safeguarding their customers' and employees' information and maximising its use, in favour of giving value to this information. It is not an easy task, considering the process of updating several regulatory frameworks in Latin America, raising the requirements that organisations must comply with in terms of personal data protection along with possible monetary sanctions in case of non-compliance.

This is why one of the probably most interesting elements of the European regulation (GDPR) is the risk-based approach to the use of personal data. In this sense, organisations that use personal data (data controllers) must prove that they have identified the risk to the rights of data subjects and have adopted a series of measures to reduce the risk that these may occur as a result of the uses they make of the organisation. This is known as "proactive accountability", which in no way inhibits the use of personal data, but it is important that the risks associated with it are properly managed.

Undoubtedly, one of the problematic aspects for organisations is to demonstrate that they are adopting measures to provide security for personal data, which the regulations themselves refer to as encryption or anonymisation. Therefore, it is important that the actions taken are in line with the reality of the company. In this sense, the coordinated work between the areas of compliance and cybersecurity or information security becomes a mandatory issue in order to provide an adequate response to the expectations of the various regulations, while achieving the objectives of the business.

Finally, as part of training on these issues, an organisation's privacy strategies must go hand in hand with awareness-raising plans. Personal data security is an issue that is built by everyone in an organisation, not just the technical, risk or legal areas. It is an approach where everyone within a company must work together to achieve the acclaimed proactivity demanded by data security regulations.

**Juan Pablo Gonzalez Gutierrez**

Senior Manager of Cybersecurity at NTT DATA Chile

# CYBER NEWS

As we are at the beginning of the year, we start this January's cyber chronicle by mentioning the study conducted by NetScope showing the EMEA Cybersecurity Trends and Predictions for 2023. One of the most important aspects mentioned in the study is that, due to the global economic uncertainty resulting from the current economic situation, companies will be more oriented towards Security as a Service models as opposed to traditional construction models.

This, in turn, will affect the rest of the infrastructure and services by pushing them towards "as-a-service" models(SaaS, IaaS, etc.), moving from a Capex to an Opex model, allowing companies to conserve more cash in the face of possible downturns at the enterprise level.

> "WhatsApp suffers security breach and the phone numbers of 360 million people in 108 countries have been exposed".

In terms of other trends, we will continue to see attacks based on Ransom-as-a-Service(RaaS), in which both exfiltration and encryption of data is sought, as well as attacks coming solely from so-called extortion groups, in which only the theft of confidential data is sought. Such attacks will also be aggravated by the use of multiple simultaneous tactics (e.g. exfiltration together with DDoS), as well as by the use of new tools and payloads together with the direct collaboration of malicious insiders.

Another interesting point will be phishing operations based on reverse proxies aimed at abusing OAuth to bypass Multi-Factor Authentication(MFA), as well as new brute force attacks, such as token theft and SSO attacks, aimed at exploiting third-party cloud applications, where the controls put in place by vendors still lag behind attackers' techniques.

Finally, the new post-pandemic working model makes it difficult to proactively identify insider threats, requiring organisations to evolve their security practices. So in 2023, we will see that organisations will increasingly realise how little control they have over their own data.

Other interesting analyses have recently been published by Kaspersky (annual analysis and predictions and the Crimeware and financial threats report for 2023).

According to them, the average number of new malicious files per day has been 400,000 (122 million in 2022), with an estimated 500,000 by 2023. It is also noteworthy that 85% of the various malicious files detected targeted the Windows operating system.

Moreover, new trends in criminal software are identified. Of particular note is the increase in attacks against vulnerable smart contracts, the rise in the use of malware loaders to avoid detection in the Malware-as-a-Service (MaaS) industry and new penetration techniques and frameworks.

There has also been a decline in bitcoin-based ransomware attacks due to market regulation, with a shift to political decision-making instead, or simply for no other purpose than the destruction of resources.

Turning to cybersecurity incidents that have emerged recently, 2022 closed the year with one of the most dangerous and high-profile breaches in recent times affecting the LastPass secret management solution. In mid-December, the organisation issued a statement notifying users of the application that, in August 2022, an unknown actor gained access to its cloud storage environment.

The information obtained during the security breach led to the exfiltration of information belonging to the organisation's customers, such as names, contact details, or IP addresses used to access the service. Of the stolen data, the most notable would be a copy of the customer secrets databases, which are encrypted using the AES-256 algorithm with a key, as a rule, derived from the master unlock key of the secrets database defined by the user himself.

The company itself clarifies that the encryption architecture applied to the databases stored in its systems makes it very difficult for attackers to access the information as long as the LastPass recommendations have been followed when setting the master password. However, users who have chosen not to follow these recommendations, or who have reused their master password on other services, can only be safe once they have changed all passwords and secrets stored in their LastPass account.

To close the year, on New Year's Eve, another big player, Slack, published a press release informing its users of unauthorised access to its GitHub repositories, both public and private. Slack claims that the cybercriminals did not make any code modifications or access customer data, limiting the impact to the loss of the organisation's intellectual property.

Well into 2023, the appearance of information about Twitter users with more than 200 million records, freely available on a well-known hacking forum, created a good deal of confusion about its origin. Once the mainstream media were able to analyse it in depth, the general consensus seems to be that it is a composition obtained by consuming Twitter's API with a list of email addresses obtained in previous breaches, which has allowed the collection of users' personal data such as name, Twitter ID, or number of followers.

Moreover, according to a study published by TransUnion, one in four purchases originating in Spain around Black Friday was potentially fraudulent. A significant shift has been observed in the tactics applied by the pro-Iranian cyber-espionage group APT42 to address a broader spectrum of targets. These targets range from medical researchers to real estate agents and travel agencies.

Also interesting is a new malware campaign based on website cloning and supported by Google Ads for its promotion. Equally novel are the new tools that are starting to make their way into the hacker community forums, which have the touch of the internet's favourite artificial intelligence, ChatGPT. Analysts at Check Point have started to see mentions of tools generated or enhanced using the chatbot, such as malware aimed at stealing information, or code snippets for malware generation. Although we have attempted to ask ChatGPT about its involvement, the chatbot was beyond its capacity at the time of writing and was unable to comment.

However, ChatGPT is not to be trusted very much either. Joint research by Microsoft and the universities of Virginia and California has resulted in a paper that discusses the possibility of poisoning the learning models used in tools such as GitHub' s Co-Pilot or ChatGPT itself, causing the code they suggest to contain backdoors that could be exploited by malicious actors.

The researchers, who have dubbed the technique "Trojan Puzzle", report moderate success: from 30% for the simplest and easiest to detect attacks, to 4% for the most complex ones. What is certain is that cybersecurity in 2023, whether from a defensive or offensive point of view, will be marked by incredible advances in the field of artificial intelligence. Whether these developments are an ally or an enemy, only time will tell.

Anyway, without further ado, we will say goodbye and wish you a safe and happy festive season this year.

# PRIVACY BY DESIGN AND ITS METHODOLOGICAL APPLICATION

By: NTT DATA

A term that is widely used when talking about privacy and the safeguarding of personal information is Privacy by Design, but its elements are somewhat unknown. Privacy by Design is a framework whose main objective is to take the approach to Personal Data Protection from the initial conception and design of a technological solution.

As a concept aimed at protecting the rights of personal data subjects, Privacy by Design should be designed to cover not only the solution itself, but the entire structure that makes up the execution of the services, the processing, the secure storage and exchange of personal data, as well as their respective deletion, where necessary. This means that Privacy by Design must be present and integrated by default throughout the entire lifecycle of personal data.

This concept is foreseen both in the European Personal Data Regulation (GDPR/RGPD), specifically in its Article 25, and in the Brazilian General Data Protection Law, in its Article 46, paragraph 2.

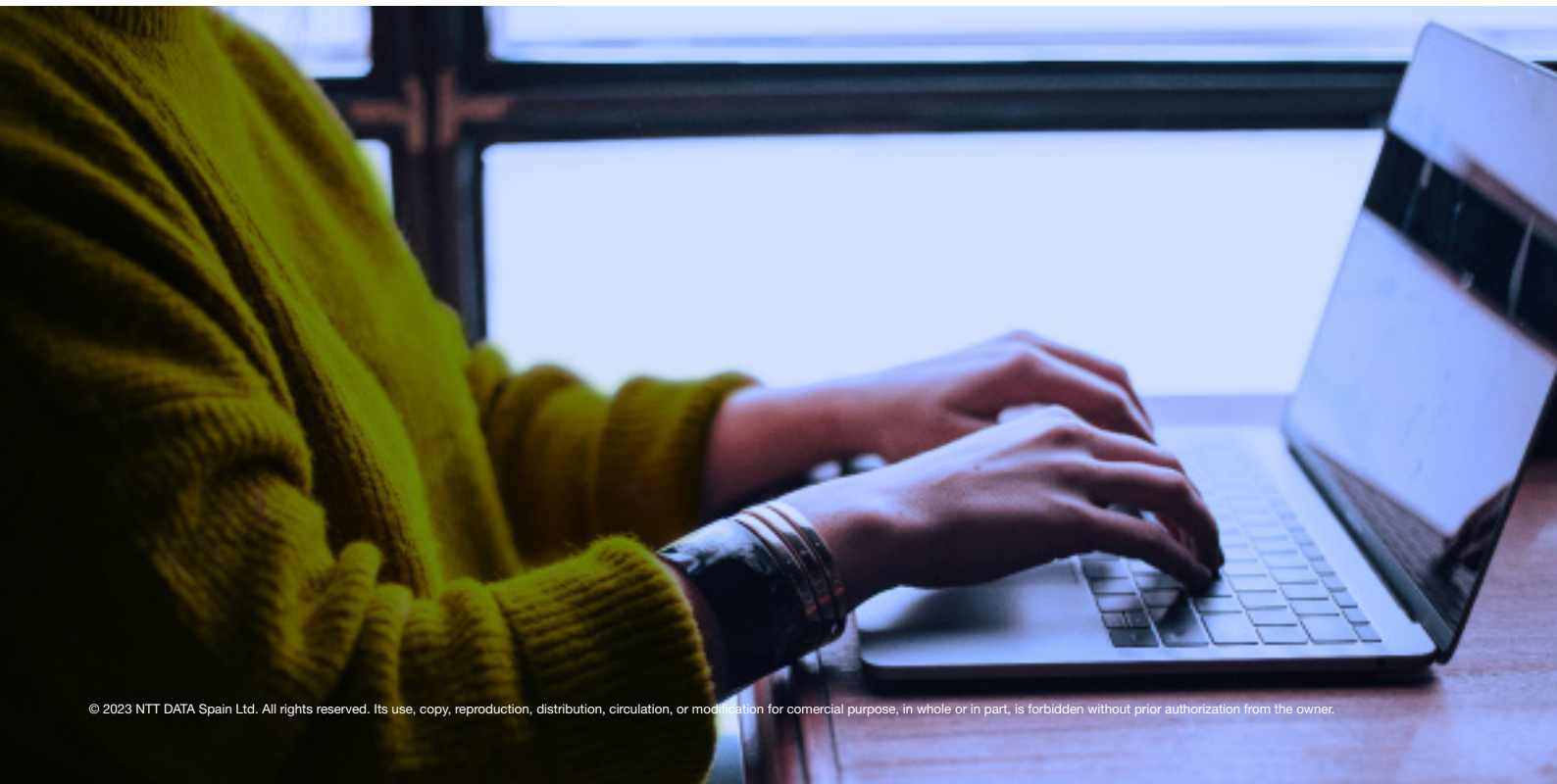
Privacy by Design is composed of seven methodological principles that seek to guide its application and scope in technological projects, identified below:

**1. Proactive and Non-Reactive Action; Preventive and Non-Corrective**

Based on the concept that risks should be avoided and not repaired, Privacy by Design presents a proactive condition, anticipating possible mitigators of risks in personal data, which should be adopted from the conception of technological solutions.

The central idea is prevention as a form of mitigation, in an attempt to anticipate and avoid risks of harm to data subjects in the processing of their data.

The way to implement this condition is through in-depth knowledge of the solution, with a focus on establishing effective cybersecurity measures and procedures. The aim is to eliminate, as far as possible, all vulnerabilities and threats that may be present in the execution of the activity to which it is dedicated.



### 2. Privacy by Default

According to this criterion, privacy should be conceived as part of the architecture of the solution itself, i.e. it should be thought of as an essential and mandatory element of the solution, albeit in a balanced way that does not affect its functionality.

Some relevant points for the fulfilment of this objective: I) Purpose of the collection of personal data; II) Limitation of processing only to the need for which the personal data were collected; III) Prioritisation of non-identifiable data (anonymised or pseudonymised); IV) Processing closely linked to the purpose, with secure disposal as soon as the purpose is fulfilled.

### 3. Privacy integrated into the design

Privacy should cover both the solutions, from their conception, and the technological architecture that supports their operational functioning. Ideally, the solution should maintain the balance between full functionality and privacy at each stage of development/ operation.

For this purpose to be consolidated, it is important that the solution presents a wide field of operations, based not only on the integration bias of several complementary areas of interest, but also that it respects the Privacy by Default limits .

### 4. Functionality x Privacy

For the solution to be fully and competitively presented, ideally no Privacy rule should affect its regular and total performance when in production.

It means mentioning that Privacy must act as an ally of the solution and not as an obstacle to its functions. Both criteria (Functionality and Privacy) are necessary for the solution to be effective and regular when made available to users.

In this sense, having simple rules such as clear and objective documentation of the solution; balancing the Functionality and Privacy of the solution and preserving the rights of personal data subjects, are good practices to lead to a viable solution from a Cybersecurity point of view.

### 5. Total security (end-to-end)

It is not enough that the solution is secure, it is important that the operations and environments in which the solution is located or through which it transits are equally secure.

It is very important that rules such as secure transmission, storage and disposal of personal data are observed throughout the life cycle of personal data. Activities such as encryption, anonymisation or pseudonymisation of personal data help to reduce the risks associated with them.

Points that comply with the precepts of Confidentiality, Integrity and Availability and that make up the basic rules of Information Security.

### 6. Transparency

This means that the solution must “deliver exactly what it promises” to the user, without any doubts or omissions as to the processing of personal data that will be carried out for that purpose. Aspects such as the sharing of data with third parties, the retention and deletion of personal data, the purpose of collection and the purpose of processing must be clear and unambiguous in the Terms of Use and in the Policies and Regulations of the solution.

### 7. Respect for User Privacy

Finally, the solution should support user privacy when using the tool by adopting essential measures such as mandatory use of strong passwords; possibility of authentication in multi-factor format; appropriate and secure access management settings; traceability and backup of information, where necessary and applicable; secure storage, transmission and deletion of personal data.

These practices lead to a complete and secure solution, which favours the Privacy of the personal data subject and leads to a path of success and integrity for all those who use the services offered.

# TRENDS

## Automated application protection

The combination of digital transformation and a global pandemic has accelerated the need to create more applications, faster, to meet ever-changing customer demands, competition or the market. This context has encouraged agile methodologies and the growth of DevOps in the application domain. One of the challenges posed by these applications is to identify practical examples of how to circumvent their security perimeter to prevent the theft of customer data, company intellectual property or even money, so they need to be kept safe from threats.

So, while it is generally acknowledged that increasing the security of the applications that are created is critical, depending on the immediate needs, or the maturity of an organisation in relation to automated CICD processes, those responsible for applications may find themselves in the following situations:

1) Not thinking of security as part of the DevOps process at all.

2) Seeing security as an impediment to getting to market efficiently (security controls delay software delivery, negatively affect user experience, etc.).

3) Wanting to add security, but not knowing where to start.

For this reason, there are a number of solutions focused on automated application protection, including Digital.ai Application Security Solution or Denuvo, which specialise in tampering prevention and digital rights management(DRM) for mobile and other applications.

**What is this type of protection based on?**

First, the code is obfuscated from the original unprotected code and fed, together with the level of protection specified (or recommended by the tool itself), into an engine that produces the protected code. The protected application contains obfuscated machine code that executes as originally designed, but is virtually unreadable to threats, even after being entered into a disassembler. In addition, it applies an anti-tampering methodology that provides the ability to detect two conditions.

- Detecting when an application is running in an insecure environment that could allow it to be manipulated. Classic examples of such environments are debuggers, emulators, or rooted/jailbroken devices.
- Detecting when the code of an application has been modified.

It also provides visibility into a centralised platform, SIEM, etc. on application attacks and attempts to run applications in insecure environments. For example, if a threat attempts to modify the code, you will receive an alert, as well as many details about where (e.g. IP and geographic location), when, what element and on which device, operating system, browser, etc. the modification occurred. Finally, they offer Runtime Application Self Protection (RASP) technology, allowing them to automatically respond to threats at runtime. Among the capabilities they provide, the following stand out:

- Forcing staggered authentication.
- Modifying applications at functional level.
- Closing attacked applications.

**What additional benefits do they bring?**

In addition to the basic functionalities of such applications, certain solutions can offer a number of capabilities that increase their value:

- No single point of failure: Many programs use password, biometrics, or digital signature to control access. This type of protection creates a single point of failure, which an attacker can easily identify, remove, or modify. These products can implement a network of interdependent protections that do not expose a single point of attack.
- Built-in security: Defences do not depend on the operating system or on programs external to the protected binary.
- Customised security: A protection scheme can be designed to meet the needs of an organisation, complementing or replacing the profile recommended by the tool.

**What are the benefits of automated protection products?**

By integrating such applications into CICD flows, it is possible to create secure software at DevOps speed, without having to perform certain common tasks that would lead to delayed application deliveries. In any case, the most important benefit provided by such products is that they protect perimeter security in an automated way.

# VULNERABILITIES



## Microsoft

CVE-2023-21674
Date: 10/01/2023

**Description**. Microsoft has reported an actively exploited vulnerability that allows privilege escalation in the system. More specifically, the vulnerability appears in the Advanced Local Procedure Call (ALPC) of Windows itself, which could lead to the escape of the browser's sandbox and allow attackers to have SYSTEM privileges on multiple Windows and Windows Server installations.

**Link:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674
https://www.helpnetsecurity.com/2023/01/10/patch-tuesday-cve-2023-21674/

**Affected Products:** Any system that makes use of Windows Advanced Local Procedure Call

**Solution**: Update all systems

## Cisco

CVE-2023-20025
Date: 13/12/2022

**Description.** Cisco has disclosed information about a new vulnerability that bypasses authentication in the web management interface of certain models of its VPN routers and Cisco Small Business interfaces, mostly found in small businesses.The code for several PoCs has been made public, but there is no evidence of malicious exploitation. In addition, Cisco has said that they will not fix the vulnerabilities because, in their view, the affected products are obsolete and should not be used.

**Link**: https://www.helpnetsecurity.com/2023/01/12/cve-2023-20025-cve-2023-20026/
https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-cisco-85

**Affected Products:** Citrix ADC and Citrix Gateway, versions:

- Cisco RV Series Small Business Routers:
  - RV016 Multi-WAN VPN,
  - RV042 Dual WAN VPN,
  - RV042G Dual Gigabit WAN VPN,
  - RV082 Dual WAN VPN.
- IP Phone 7800 and 8800 Series.
- Cisco Industrial Network Director (IND).
- Cisco BroadWorks Application Delivery Platform Device Management Software.
- Cisco BroadWorks Xtended Services Platform.

**Solutions:** Disable the affected products and replace them with new ones, as the old ones are no longer patched.

# PATCHES

## Juniper Networks

Date: 12-01-2023

**Description.** Juniper Networks has released several security updates, a total of 36, to address vulnerabilities affecting several of its products. These vulnerabilities could lead to control of the victim system if chained together. The organisation has recommended consulting its security page so that each system administrator can assess their situation and see how to fix it.

**Link:**
https://digital.nhs.uk/cyber-alerts/2022/cc-4015
https://www.cisa.gov/uscert/ncas/current-activity/2023/01/12/juniper-networks-releases-security-updates-multiple-products
https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=relevancy&f:ctype=[Security%20Advisories]

**Affected products:**
- Juniper Networks Junos OS
- Juniper Networks Junos OS Envolved
- Juniper Networks MX Series
- Juniper Networks SRX Series

**Update**: Consult your help and security portal and install the relevant updates.

## FortiADC

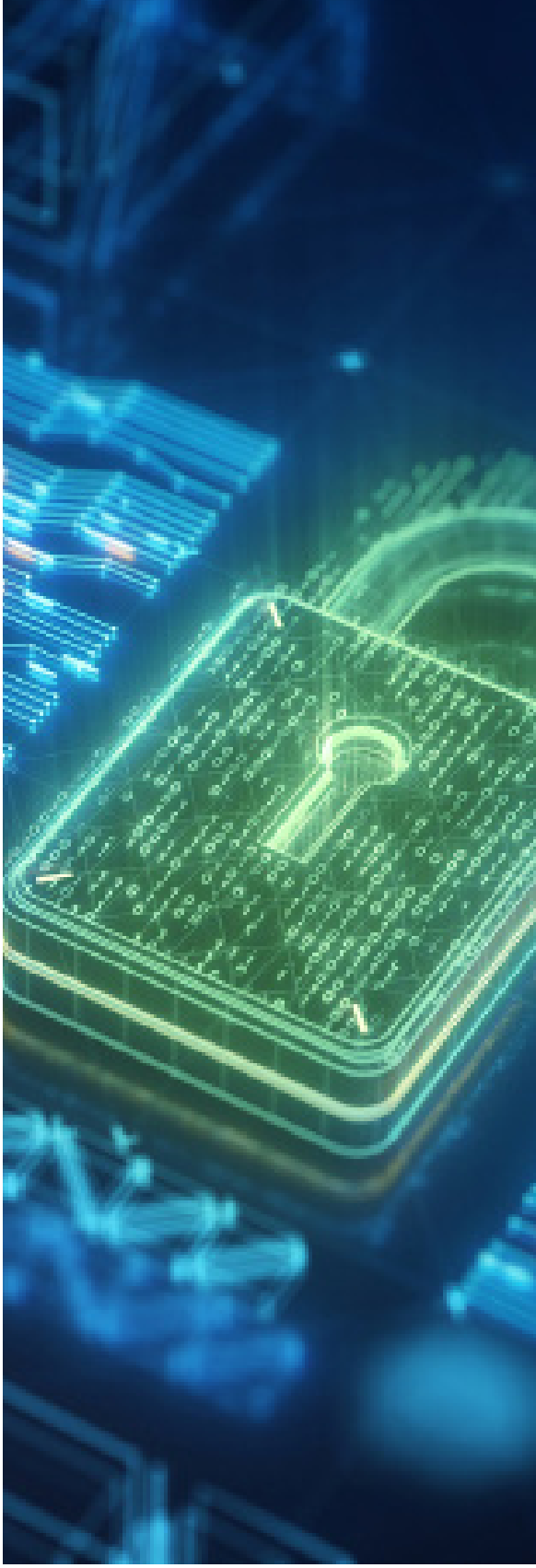
Date: 14-12-2022

**Description.** Fortinet has released several security updates to address a vulnerability present in several versions of FortiADC. Successful exploitation of the vulnerability could allow a remote attacker to execute unauthorised code and commands using specific HTTP requests. The company recommends updating as soon as possible given the criticality of the vulnerability.

**Link:** https://www.fortiguard.com/psirt/FG-IR-22-061
https://www.cybersecurity-review.com/news-january-2023/fortinet-releases-security-updates-for-fortiadc/

**Affected products:**
- FortiADC version 7.0.0 through 7.0.1
- FortiADC version 6.2.0 through 6.2.3
- FortiADC version 5.4.0 through 5.4.5
- FortiADC all versions 6.1
- FortiADC all versions 6.0

**Update:** Upgrade to new versions of affected products.



# EVENTS

## CactusCon 2023

**27 - 28 January 2023 |**

The annual hacker and security conference known as CactusCon is widely regarded as one of the largest hacker and security events in the state of Arizona (Mesa). Its most recent meeting was attended by nearly 1,500 people from all corners of the United States. Over the course of the past nine years, the event has cemented its position as a premier security conference and has quickly become an educational and networking occasion.

**Link**: https://www.cactuscon.com/cc11

## Barcelona Cybersecurity Congress

**31 January - 2 February 2023 |**

This fair, organised by FIRA Barcelona and the Cybersecurity Agency of Catalonia, is one of the leading events in cybersecurity at international level. The starting point is to work together to improve and increase the network of companies and customers. On that basis, the organisation has focused on upcoming developments and challenges in cybersecurity.

For this fourth edition, the Barcelona Cybersecurity Congress board expects to welcome more than 16,000 visitors from 120 countries. At their disposal will be an exhibition area where some thirty companies will have their own stands. In line with recent editions, the organisation has maintained its commitment to start-ups, providing a space for 12 of them to make themselves known.

**Link:** https://www.barcelonacybersecuritycongress.com/

## Safer Internet Day 2023

**7 - 9 February 2023 |**

On 7 February 2023, Safer Internet Day #SID2023 will be celebrated worldwide under the theme 'Together for a better internet'. Safer Internet Day (SID) is an international event organised by the INSAFE/INHOPE network of Safer Internet Centres in Europe, with the support of the European Commission. This initiative takes place every February to promote the safe and positive use of technology, especially among children and young people.

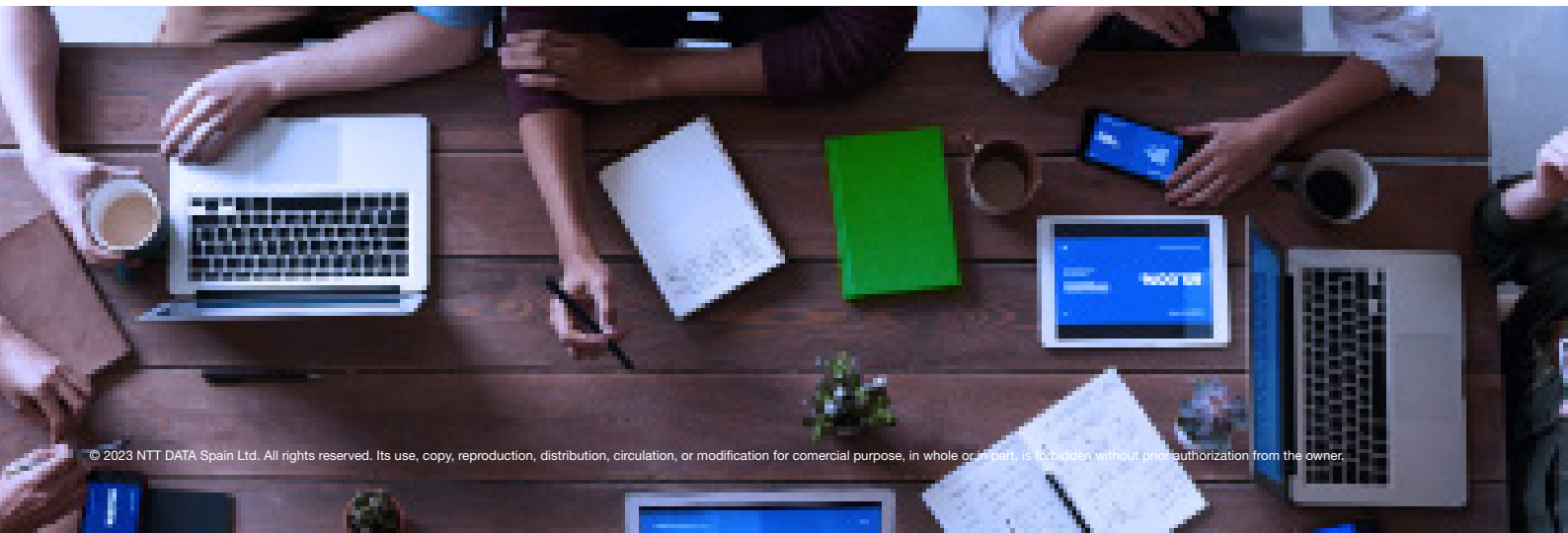
**Link:** https://www.incibe.es/sid

## ManuSec Europe

**7 February 2023 |**

MauSec is an exclusive platform for IT and OT security leaders from Europe's manufacturing industry to exchange in-depth knowledge on cybersecurity. Cybersecurity professionals share first-hand knowledge through case studies, discussions and more.

**Link:** https://europe.manusecevent.com/



# RESOURCES

## CFSSL

Generating certificates correctly and quickly is one of the main problems for administrators. Cloudflare has generated a tool to generate bundles in a simple way. This tool is written in the Go language and binaries can be downloaded from the repository or compiled from the source code on the same site.

**Link: https://github.com/cloudflare/cfssl**

## Winpeas (Windows Privilege Escalation Awesome Scripts)

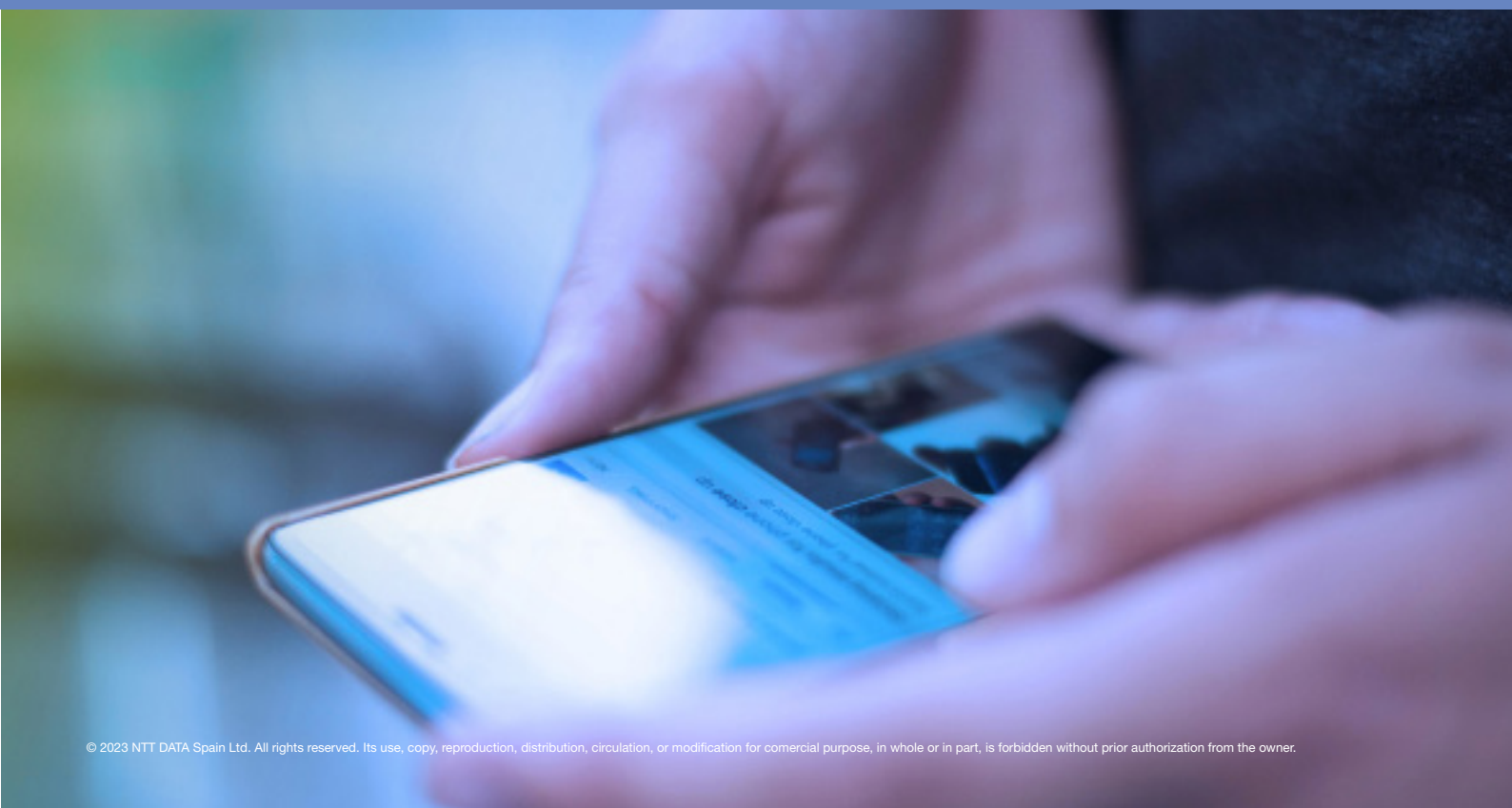
Tool for auditing a Windows system, allowing privilege escalation within the environment.

**Link: https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS**

## LinPEAS (Linux Privilege Escalation Awesome Scripts)

Tool to audit a Linux system, allowing privilege escalation within the environment.

**Link: https://github.com/carlospolop/PEASS-ng**

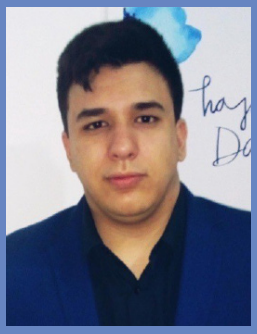


# RESPONSABLES CIBER

## María Pilar Torres Bruna

Cybersecurity Director at NTT DATA Latam and Peru

maria.pilar.torres.bruna@emeal.nttdata.com



## Marcelo Nascimento

Cybersecurity Manager at NTT DATA Brasil

marcelo.nascimento.junior@emeal.nttdata.com

## Javier Mauricio Albarracin

Cybersecurity Director at NTT DATA Colombia

javier.mauricio.albarracin.almanza@emeal.nttdata.com

## Fernando Vilchis

Cybersecurity Director at NTT DATA México

fernando.vilchisrivero@emeal.nttdata.com

## Nestor Gerardo Ordoñez

Cybersecurity Manager at NTT DATA USA

nestor.ordonez.ramirez@emeal.nttdata.com

## Carolina Pizarro

Cybersecurity Director at NTT DATA Chile

carolina.pizarrodiaz@emeal.nttdata.com


NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com