NUMBER 79 | JUNE 2023

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

WILL WE HAVE AGI (ARTIFICIAL GENERAL INTELLIGENCE) BY THE END OF 2023?

Developer Sigi Chen, citing unnamed sources, tweeted a few weeks ago "*I was told that GPT-5 is scheduled to complete training this December and that OpenAI expects it to reach AGI*".

But what exactly is AGI?

AGI or General Artificial Intelligence is when an AI learns and understands tasks or concepts commonly performed by humans. Unlike specialised or narrow AI, which focuses on specific tasks and is designed for a particular purpose, AGI can adapt and tackle new and unfamiliar problems, showing a level of autonomy and cognitive flexibility similar to that of humans. Unlike artificial intelligence, which relies on ever-expanding data sets to perform more complex tasks, AGI will exhibit the same attributes as those that relate directly to the human brain - it is described as a type of AI that can understand, learn, and perform intellectual tasks in much the same way as the human brain. **In other words, AGI is the ability of AI to learn in the same way as humans.**

AI refers to a machine that can copy human cognitive abilities, such as problem solving and learning. But a human must first program the machine so that it can learn from past patterns to create new information or solve a problem. Whereas AI is pre-programmed to perform a task that a human can perform (but more efficiently), AGI expects the machine to be as intelligent as a human. To date, AGI is a goal in artificial intelligence research, but it has not yet been achieved.

Like all technologies, AGI has its good side (increasing productivity by speeding up AI-enabled processes and freeing humans from repetitive work, boosting the global economy or helping to bring about new scientific discoveries) and its "unintended or less good" side (spread of extremely convincing human-like bots on social media platforms, concentration of this technology in a few hands, labour displacement, misuse).

Precisely to avoid the latter undesirable effects, more work needs to be done to make these systems more accurate, secure, interpretable, and transparent by working with legislators to promote the development of robust AI governance systems. These should include at a minimum: new and capable regulatory authorities dedicated to AI, as well as oversight and monitoring of high-capacity AI systems and large volumes of computational capacity. In this regard, we already have some initiatives such as the **Artificial Intelligence Act (AI Act)**, which is a regulation proposed on 21 April 2021 by the European Commission that aims to introduce a common regulatory and legal framework for artificial intelligence, but it is clear that further efforts are needed.

Whether or not ChatGPT 5 will finally achieve AGI remains to be seen, as with other cutting-edge technology issues such as quantum supremacy (the point at which a quantum processor is able to perform a task that cannot be performed by any classical computer in a reasonable amount of time). There are opinions of all kinds, from those who think that it has already been achieved (in particular by Chinese scientists) to those who, much more sceptical, think that it will never be achieved. What is certain is that there are a lot of people and effort behind all these issues, and at least with respect to the AGI, we may find out by the end of this year through ChapGPT-5! Hopefully by then, the position OPEN AI advertised a few days ago for a "**kill switch engineer**" (or shutdown switch) who would be responsible for shutting down servers in the event of a catastrophe will have been filled…

María Pilar Torres Bruna

Cybersecurity Director at NTT DATA Europe & Latam

CYBER NEWS

We begin this new edition of RADAR with the following message: online security remains a constant concern for businesses and users around the world. Recently, social media consultant and analyst Matt Navarra reported on Twitter that hackers had hacked into verified Facebook pages to post ads distributing malware.

One of the hacked sites, Meta Ads, tricked users into downloading a 'more professional and secure' administration tool due to browser security issues. However, instead of downloading a legitimate tool, the link redirected users to a malware-infected web page. The other hacked page purported to be Google AI and directed users to fake links to Google's artificial intelligence chatbot. Both pages were able to buy Facebook ads and distribute suspicious download links.

> "It is therefore important never to rely on links to supposedly official websites sent to you by email or SMS".

Fortunately, both hacked pages were deactivated, and Meta launched a verification program called 'Meta Verified' to increase the security of the platform. However, Facebook and Instagram users who wish to have proactive account protection will have to pay a minimum of twelve euros per month.

This incident highlights the importance of online security and the need for companies to implement stronger security measures to protect their users from cybercriminals. Nevertheless, it is not only the security of social media platforms that we need to take into account.

With tax season underway, scammers are also taking the opportunity to trick people through mass mailings and messages with scams in which they try to trick someone into falling for the trap. These attacks, known as phishing attacks, consist of sending out mass messages as if they were casting hundreds of thousands of hooks, in the hope that someone will take the bait.

Scammers use deceptive tactics, often claiming that the tax authorities will give you money back. These messages may also include links to fraudulent websites that look official, but are designed to steal personal information, such as card numbers and security codes. These websites are forgeries that use Treasury logos and fonts to look like an official website. It is advisable to manually search the official website of the Tax Agency and authenticate yourself from there to look for possible notifications. In short, online security remains a constant concern. With tax season underway, it is important to be cautious and vigilant about the emails and messages we receive, as many of them may be fraudulent. Businesses must also implement stronger security measures to protect their users from hackers.

Also noteworthy is the following news. The National Institute of Cybersecurity (INCIBE) is warning about a new fraudulent tactic in which the identity of the Social Security is impersonated by means of smishing.

The purpose of this scam is to obtain victims' personal data through a fraudulent website containing a form. The text messages indicate that the healthcare card needs to be updated using the link attached in the body of the message.

If the user clicks on the URL, they will be redirected to a malicious website that asks them to fill out a form with the following information: first name, last name, email address and date of birth. Once this data is entered, cybercriminals will have access to all the information necessary to carry out cyber-attacks and deceive victims.

On the other hand, INCIBE warns that it does not rule out the existence of other similar campaigns through emails requesting the same information. In addition, the text messages reported so far contain spelling errors in their wording, raising suspicions about their authenticity.

In another curious piece of news, now that the use of AIs, and ChatGPT in particular, is all the rage, Meta has come to light and has detected links on the web to apps pretending to be ChatGPT with malware.

Meta has revealed some of the actions taken during the first quarter of 2023 to address the threats detected in its applications targeting individuals and businesses. These threats include malware campaigns in which cybercriminals spoof ChatGPT applications, as well as the identification of nine antagonistic networks involved in cyber espionage operations.

In its statement on the website, Meta details that one of the most prominent attack types during this period has been malware campaigns in which cybercriminals exploit popular themes, such as generative Artificial Intelligence (AI) technology with ChatGPT, to get users' attention.

Specifically, the company reports that, since March, its analysts have identified around ten different malware families that spoof ChatGPT applications and similar tools. Campaigns related to cryptographic scams have also been detected.

In these campaigns, malicious actors created malicious browser extensions available in official web shops, offering fake AI-related tools. Sometimes these extensions even included real ChatGPT functions along with the malware, in order to camouflage themselves and avoid arousing suspicion. However, Meta's team of researchers managed to block more than a thousand malicious extensions of these malware campaigns to prevent users from sharing them in their applications. The company also reported these malicious campaigns to other file-sharing applications in the industry, so that they can also take appropriate action.

A new scam has also been detected which involves impersonating the company FedEx to extract customers' bank details. The scam is carried out by sending a fraudulent email in which, with the excuse of paying a fee to receive a FedEx package, it redirects via a link to a survey and two forms requesting personal and bank details.

If the recipient has received an email message purporting to be from FedEx, asking them to make a payment to receive a package, but has not shared their personal information, it is recommended that the user mark the email as spam and delete it from their inbox.

HOW CAN AIS HELP IN THE DAILY WORK OF A CYBERSECURITY EMPLOYEE AND WHAT ROLE DO THEY PLAY?

By: NTT DATA

Artificial intelligence (AI) is a branch of computer and information science that focuses on developing systems or programs that can perform tasks that generally require human intelligence, such as learning, perception, reasoning and problem solving. AI systems use techniques and algorithms that allow them to learn from experience and improve their performance over time. These techniques include for example machine learning, natural language processing, computer vision and robotics, among many others.

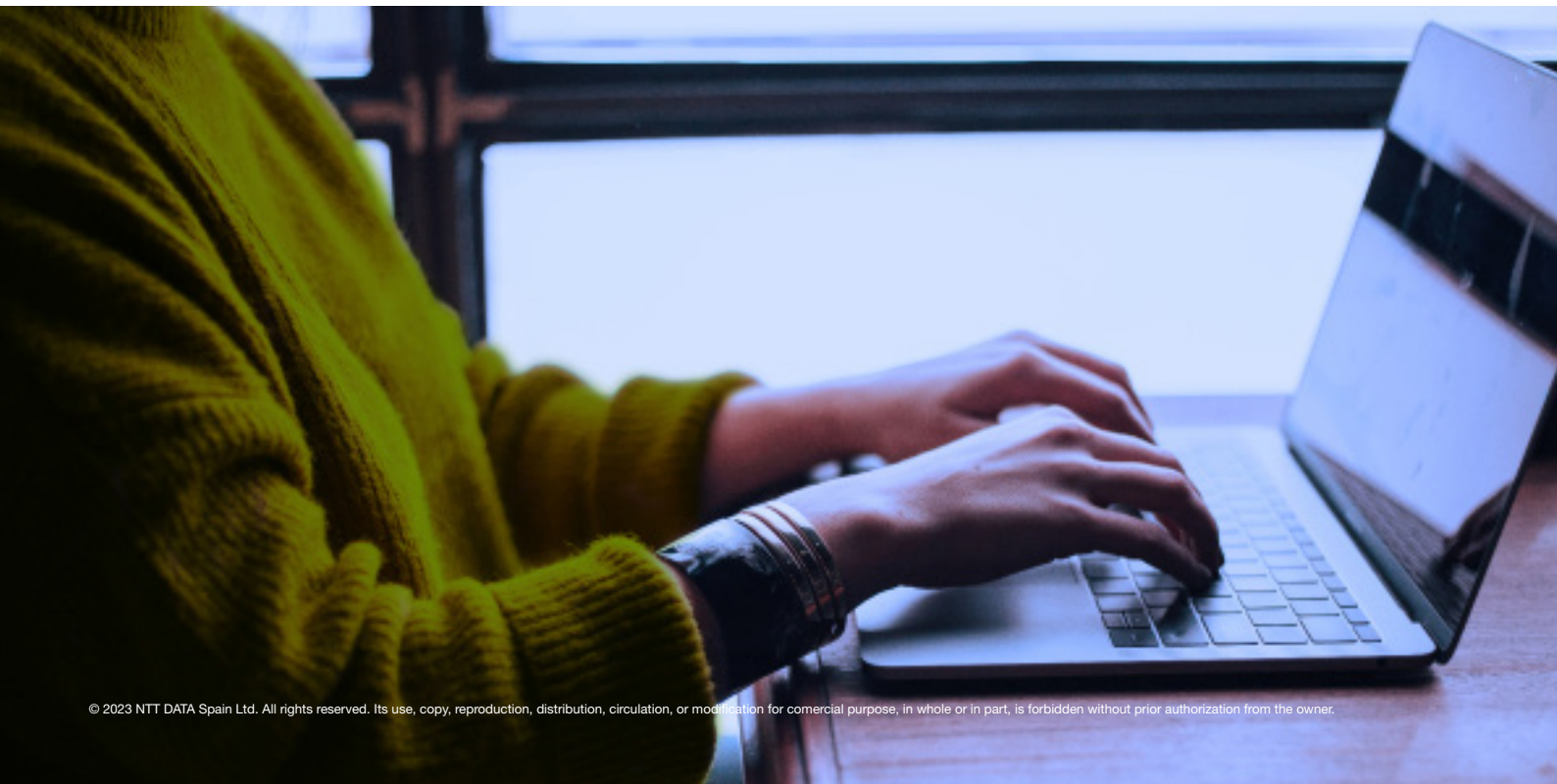
AI is applied in a wide variety of fields, such as medicine, education, industry, commerce, and entertainment. Its potential to improve efficiency and quality of life is enormous, but it also raises important ethical and social challenges that need to be addressed.

What types of AIs currently exist?

Although when we think of artificial intelligences, ChatGPT or DALL-E 2 come to mind, they are not the only ones. There are several types of artificial intelligence, each with its own approach and application. Some of the most common types of AI include:

- **Expert systems:** are systems that use specific knowledge of human experts in a given field to make decisions and perform tasks. They are used in fields such as medicine, engineering, and business management.
- **Machine learning:** is a type of AI that uses algorithms to allow systems to learn and improve through experience. It is used in applications such as fraud detection, pattern recognition and decision making.
- **Neural networks:** are AI systems that mimic the structure and functioning of the human brain. They are used in image and speech recognition applications, as well as in real-time decision making.
- **Natural language processing:** a type of AI that allows systems to understand and respond to human language. It is used in applications such as chatbots and virtual assistants.
- **Robotics:** is a field of AI that focuses on the development of intelligent, autonomous robots that can perform physical tasks in complex environments.

Each type of AI can give rise to a myriad of different applications as each can be trained to perform different functionalities.



How are they trained in cybersecurity?

Artificial intelligences (AI), such as ChatGPT, are not necessarily designed specifically for the cybersecurity domain, but they can be trained to perform cybersecurity-related tasks.

Training an AI for cybersecurity involves teaching it to recognise patterns and anomalies in data, and to make decisions based on that information. This is achieved through feeding the AI with large amounts of security data, such as network activity logs, security event logs, application logs and known threat data.

Once AI has been trained to identify patterns and anomalies, it can be applied to various cybersecurity tasks, such as intrusion detection, malware identification, network activity monitoring, malicious behaviour prediction, and automatic response to security events.

To maintain an effective cybersecurity IA, it needs to be regularly updated with new threat data and techniques. It is also important that decisions made by AI are monitored and adjusted as necessary to ensure accuracy and effectiveness in the protection of IT systems and data.

For ChatGPT, the GPT-3.5 model is trained on a large amount of unstructured data from different sources, including web pages, books, news articles, forums, and social networks, with the aim of learning patterns and associations in natural language. Through this continuous training, the model becomes increasingly accurate and effective in its ability to understand and generate natural language.

How can these AIs help cybersecurity profiles?

Artificial intelligences can help cyber security profiling in multiple ways by analysing large amounts of security data in real time, identifying patterns and anomalies, and making automated decisions to detect and respond to security threats.

Here are some ways in which artificial intelligences can help cybersecurity profiles:

1. **Threat detection:** AI can analyse large amounts of security data in real time and detect suspicious patterns or behaviour in network activity or computer systems. By identifying these behaviours, AI can alert security teams to investigate and respond to the threat.
2. **Vulnerability scanning:** AIs can scan systems and applications for known or unknown vulnerabilities. Security teams can use this information to identify and fix vulnerabilities before they are exploited by attackers.
3. **Malware identification:** AIs can analyse software behaviour patterns and detect malware that has infiltrated a computer system. This can help security teams quickly identify the threat and take action to mitigate it.
4. **Security incident management:** AI can assist in security incident management by providing a rapid and automated response to security events. For example, AI can take action to stop an attack or block suspicious behaviour while the security team investigates the incident.
5. **Continuous monitoring:** AI can continuously monitor network activity and computer systems to detect and respond to threats in real time. This can help security teams maintain a more proactive and effective security posture.

In short, AI can assist cybersecurity profiles in threat detection, vulnerability analysis, malware identification, security incident management and continuous monitoring. By automating these tasks and enabling a faster and more accurate response to security events, AI can significantly improve an organisation's security posture.

ARTIFICIAL INTELLIGENCE APPLICATIONS IN CYBERSECURITY

By: NTT DATA

Cybersecurity has become a major concern for individuals, businesses, and government institutions around the world. With the increasing amount of data and devices connected to the network, cybercrime has increased exponentially in recent years. Fortunately, artificial intelligence (AI) can be a valuable tool in the fight against cybercrime.

AI has the potential to revolutionise cybersecurity in many ways. Firstly, machine learning algorithms can analyse large amounts of data to identify patterns and anomalies in network traffic and activity logs. These patterns can assist and alert security professionals before an incident occurs that puts the organisation's infrastructure at risk.

In addition, AI can be used in virus scanning engines and to improve malware detection. Machine learning algorithms can analyse the code of a program and compare the sample with a known data set to determine if it is malware. These algorithms can detect patterns of behaviour on systems that indicate malware infection.

Another important application of AI in cybersecurity is the identification of insider threats. Often, cyber-attacks can come from within the organisation itself, either through negligence or intentionality. AI can analyse employee behaviour patterns to detect suspicious activity and alert professionals.

AI can also be used to improve authentication and user identification. AI-based authentication systems can analyse user behaviour, such as typing patterns and the way they interact with the user interface, to determine whether a user is legitimate or an impostor.

Ultimately, AI can help improve security incident response capability by integrating it with automation mechanisms. AI systems can be programmed to take immediate action when suspicious behaviour is detected, such as disconnecting a device from the network or blocking access to an account. This can help prevent damage before it occurs and limit the spread of the attack.

Despite the potential benefits of AI in cybersecurity, there are also concerns about its use. In particular, privacy and ethics are important issues to consider. AI can be used to collect and analyse large amounts of user data, which raises privacy concerns. This may include the implementation of clear and transparent policies on the use of AI, as well as the adoption of sound privacy and security practices.

Another concern is the possibility of attackers using AI to carry out more sophisticated cyber-attacks.

In addition, AI systems used in cybersecurity must be rigorously tested and evaluated to ensure their effectiveness and reliability. Security profiles must work in collaboration with AI developers to ensure that systems are able to detect a wide range of threats and adapt to new risks as they emerge.

There are a number of cybersecurity tools that use artificial intelligence to improve their effectiveness in detecting and preventing cyber-attacks. Examples of such tools include the following:

1. **Darktrace:** This tool uses machine learning algorithms to analyse network traffic patterns and detect threats in real time. It is able to detect even the most sophisticated threats, such as zero-day attacks and insider threats.
2. **Cylance:** It is an Endpoint Protection Platform (EPP) tool that uses artificial intelligence to identify and prevent malware attacks. The tool uses a machine learning engine to analyse the code of programs and determine whether they are malicious or not.
3. **Palo Alto Networks:** It can be used to improve threat detection and attack prevention. The tool uses machine learning algorithms to analyse network traffic and detect suspicious patterns.
4. **McAfee:** It uses artificial intelligence to improve detection and prevention of malware attacks and insider threats. The tool uses machine learning algorithms to analyse user behaviour and detect suspicious activity.

It is important to stress that AI is not a perfect solution for cybersecurity. While it can help detect and prevent attacks, it cannot completely replace qualified professionals. It should be used as a complementary tool to improve the effectiveness of cybersecurity and not as a stand-alone solution.

TRENDS

CYBERSECURITY OF THE INTERNET OF THINGS (IOT)

The Internet of Things (IoT) has revolutionised the way we interact with our homes and devices. However, this innovation also presents significant risks to our privacy and security. The growing number of IoT devices, estimated to exceed 55 million by 2023, presents numerous security challenges.

Many of these devices do not have adequate security features, and those that do are often not properly configured and maintained by users, leaving the door open to potential security breaches.

In addition to security, privacy is also a big issue in IoT. Smart devices collect data about users, including personal information such as the layout of their home and their daily habits. Often, this data is sent to third parties other than the original manufacturer, which can be a concern for those worried about their privacy. Despite these risks, it is possible to control the devices' access to data, although this may limit the functionality of the devices.

IoT devices can also have negative impacts on the security of businesses, as the data stored is often more sensitive and businesses have a legal responsibility to protect it. However, many companies are unaware of the security risks of IoT. There have been cases of hackers accessing databases through IoT devices, such as in one casino where hackers were able to access 10 GB of data through the aquarium thermostat. The healthcare and manufacturing sectors are particularly vulnerable, as the IoT devices used can affect the safety and privacy of patients and production processes.

Now that you have an idea of how vulnerable IoT devices can be, what measures or recommendations can be taken?

- Consider whether it is necessary to have the devices connected all the time.
- Create a separate network just for IoT devices and protect it with a secure password, update firmware and close ports that are common transmission vectors.
- Use strong and unique passwords for IoT devices, change factory passwords and enable multi-factor authentication if possible.
- Frequently check for and apply security updates for IoT devices.
- Use anti-malware software that specifically protects IoT devices.

In short, security and privacy are critical issues in IoT that must be properly addressed to ensure that users can enjoy the many benefits that this technology offers.

VULNERABILITIES

Gitlab

CVE-2023-2478
Date: 05/05/2023

Description. On 8 May, Gitlab released a security update triggered by a critical vulnerability found in multiple versions of Gitlab Community Edition (CE) and Gitlab Enterprise Edition (EE). This vulnerability has been assigned the identifier CVE-2023-2478. Through its exploitation and if certain circumstances are met, a Gitlab user could use a GraphQL endpoint to attach a malicious executable to any project. This security flaw occurs due to incorrect assignment of permissions to access critical system resources.

Link: https://about.gitlab.com/releases/2023/05/05/critical-security-release-gitlab-15-11-2-released/#malicious-runner-attachment-via-graphql
https://www.incibe.es/incibe-cert/alerta-temprana/avisos/vulnerabilidad-en-community-edition-ce-y-enterprise-edition-ee-de-gitlab

Affected Products: This vulnerability affects the following versions of Gitlab Community Edition (CE) and Gitlab Enterprise Edition (EE)

- from 15.4 to 15.9.7,
- from 15.10 to 15.10.6,
- from 15.11 to 15.11.2.

Solution: The main workaround for this vulnerability is to update to the latest versions, as appropriate:

- 15.11.2
- 15.10.6
- 15.9.7

Aruba

CVE-2023-22779,-22780,-22781,-22782,-22783,-22784,-22785,-22786,-22787,-22788, -22789, -22790,-22791
Date: 09/05/2023

Description. A total of 13 vulnerabilities have been discovered in Aruba products, 8 of them of critical severity, 4 high and 1 medium. Those categorised as high severity correspond to multiple remote command injection vulnerabilities and a denial of service vulnerability. On the other hand, the 8 critical vulnerabilities consist of a buffer overflow present in multiple services used by the Aruba Access Point Management Protocol (PAPI). By exploiting it, an attacker could remotely execute code with administrator permissions. Finally, the medium severity vulnerability would allow an attacker to disclose sensitive information on a Wi-Fi network with a specific configuration. However, the scenarios in which exploitation of this vulnerability can occur are complex and depend on factors beyond the attacker's control.

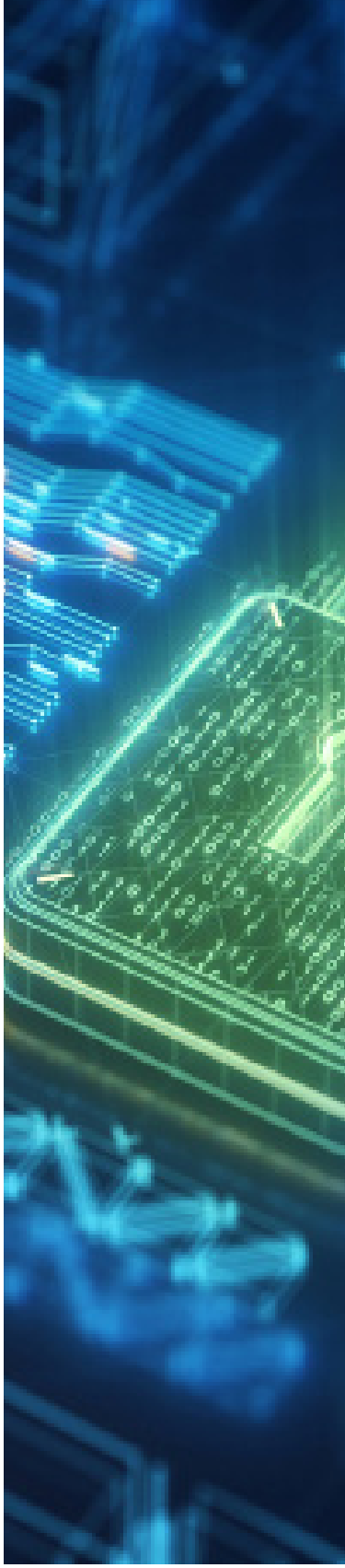
Link: https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt%20
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-aruba-products-could-allow-for-arbitrary-code-execution_2023-049

Affected Products: Aruba Access Points with InstantOS and ArubaOS 10 software:

- ArubaOS 10.3.x: versions 10.3.1.0 and earlier;
- Aruba InstantOS 8.10.x: versions 8.10.0.4 and earlier;
- Aruba InstantOS 8.6.x: versions 8.6.0.19 and earlier;
- Aruba InstantOS 6.5.x: versions 6.5.4.23 and earlier;
- Aruba InstantOS 6.4.x: versions 6.4.4.8-4.2.4.20 and earlier.

Solutions: Aruba Network has issued security updates for the affected products, so it is recommended to upgrade to the latest version available.

PATCHES



Microsoft

Date: 09-05-2023

Description. Microsoft has released a series of security updates for the month of May 2023 where it fixes a total of 38 known vulnerabilities: 6 critical remote code execution vulnerabilities, 33 high, 1 moderate and 9 not severely rated. These include three zero-days, two of which are actively exploited:

- CVE-2023-29336: this vulnerability, present in the Win32k Kernel, allows an attacker to obtain SYSTEM permissions, the highest level of privileges within a Windows system.
- CVE-2023-24932: Using this vulnerability, an attacker with administrator permissions or physical access to the computer could install a malicious boot policy. This type of malware, called UEFI bootkits, is invisible to security tools because it executes at the initial stage of the computer boot.
- CVE-2023-29325: This vulnerability would allow an attacker to remotely execute code on the computer via specially crafted emails.

Link:
https://msrc.microsoft.com/update-guide/releaseNote/2023-May
https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-may-9-2023_2023-048

Affected products: Some of the products affected are: Microsoft Bluetooth Driver; Microsoft Edge (Chromium-based); Microsoft Office Excel;Microsoft Office SharePoint;Microsoft Office Word;Microsoft Teams;Visual Studio Code; Windows Secure Boot; Windows Win32K. The full list of affected products can be found at the following link: https://msrc.microsoft.com/update-guide

Update: It is recommended to update the relevant products to the latest available version.

SAP

Date: 09-05-2023

Description. SAP has released the monthly security patch, which fixes a total of 25 known vulnerabilities: 2 critical, 9 high, 10 medium and 3 low severity, in addition to the recurring SAP Business Client update, which introduces the latest Chromium patches. These include information disclosure vulnerabilities, privilege escalation, denial of service or memory corruption. Further details about the critical vulnerability affecting the BusinessObjects Business Intelligence Platform are provided below: CVE-2023-28762: Using this vulnerability, an attacker with administrator permissions could obtain the login token of any user without any interaction from the user. Once the token has been obtained, the attacker could impersonate the user and access or modify information, as well as prevent partial or full operation of the system.

Link: https://onapsis.com/blog/sap-patch-day-may-2023
https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-de-sap-de-mayo-de-2023

Affected products: The products affected are the following: SAP 3D Visual Enterprise License Manager, version 15; SAP BusinessObjects Intelligence Platform, versions 420 and 430; SAP AS NetWeaver JAVA, versions SERVERCORE 7.50, J2EE-FRMW 7.50 and CORE-TOOLS 7.50; SAP IBP EXCEL ADD-IN, versions 2211, 2302 and 2305; SAP PowerDesigner (Proxy), version 16.7; SAP Commerce, versions 2105, 2205 and 2211; SAP GUI for Windows, versions 7.70 and 8.0; SAP Commerce (Backoffice), versions 2105 and 2205; SAPUI5, versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757 and UI_700 20.

Update: Apply the patches and updates published on the manufacturer's official website for each of the affected products.

EVENTS

XII GAP Security Symposium

22 - 29 May 2023 |

The Airport Group (GAP) with the support of Segurilatam, and the collaboration of the Federal Aviation Agency (AFAC) has organised the XII GAP Security Symposium in Guadalajara, Mexico. This event will be limited to 300 places, and attendance is by personal invitation only. The topics to be discussed at this congress will be AVSEC systems, perimeter protection, private security services and cyber threats.

Link: https://www.segurilatam.com/agenda/xii-simposium-de-seguridad-gap_20230303.html

Cyber Security International Radar (CSI Radar)

12 - 16 June 2023 |

Medina Media Events will organise the Cyber Security International Radar' (CSI Radar) event in Seville. This event will be held from 12 to 16 June, where visibility will be given to all projects and solutions at national and international level to improve security in companies, institutions, and individuals. This is a hybrid agenda, with two on-site days (Palacio de Exposiciones y Congresos de Sevilla) and three virtual days, bringing together more than 40 presentations.

LInk: https://csiradar.com/

III Congress on Digital Security and Cyber Intelligence: C1b3rwall

20 - 22 June 2023 |

The III Congress on Digital Security and Cyber Intelligence (C1b3rwall) begins on 20 June and will last until 22 June. The event is organised by the University of Salamanca and the National Police at the National Police School in Ávila. This congress was born in 2019, and the last edition brought together more than 5000 professionals related to information and communication technology, security forces, armed forces, university professors and students.

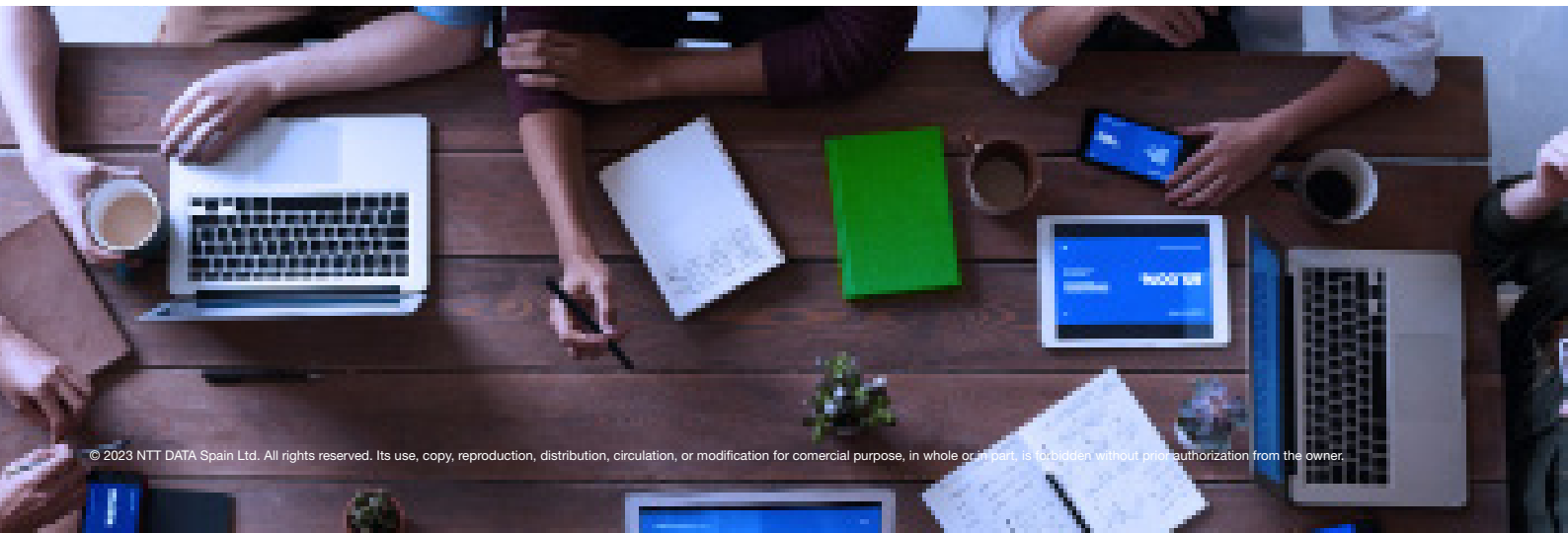
Link: https://c1b3rwall.policia.es/congreso

15 Integral Security Meeting (Seg2)

22 June 2023 |

This meeting, organised by the magazines Red Seguridad and Seguritecnia, will take place on 22 June. The event will be entitled "The New Security Paradigm: Responding to Geopolitical Challenges". This event will be a TV experience. Some of the topics to be covered are, Ukraine and digital warfare, cyberspace dangers, regulations (5G, NIS2...) inspections and management.

Link: https://www.seguritecnia.es/agenda/15-encuentro-de-la-seguridad-integral-seg2_20230104.html



RESOURCES

BGP Boofuzzer

It is an open source tool to find vulnerabilities in the BGP implementation. This tool will allow companies to assess the security of the BGP suites they use internally, as well as to use it to discover new vulnerabilities in BGP implementations by researchers.

Link: https://noticiasseguridad.com/tutoriales/bgp-boofuzzer-herramienta-para-encontrar-vulnerabilidades-en-la-implementacion-de-bgp/

Goose Tool

It is a free tool that can help network defenders identify potential malicious activity in Microsoft Azure, Azure Active Directory and Microsoft 365 environments. The tool provides new authentication and data collection methods for use in the process of defending such environments.

Link: https://noticiasseguridad.com/tutoriales/la-mejor-herramienta-gratuitita-para-la-deteccion-de-incidentes-ciberneticos-en-microsoft-azure-azure-active-directory-y-microsoft-365/

Microsoft announces Security Copilot

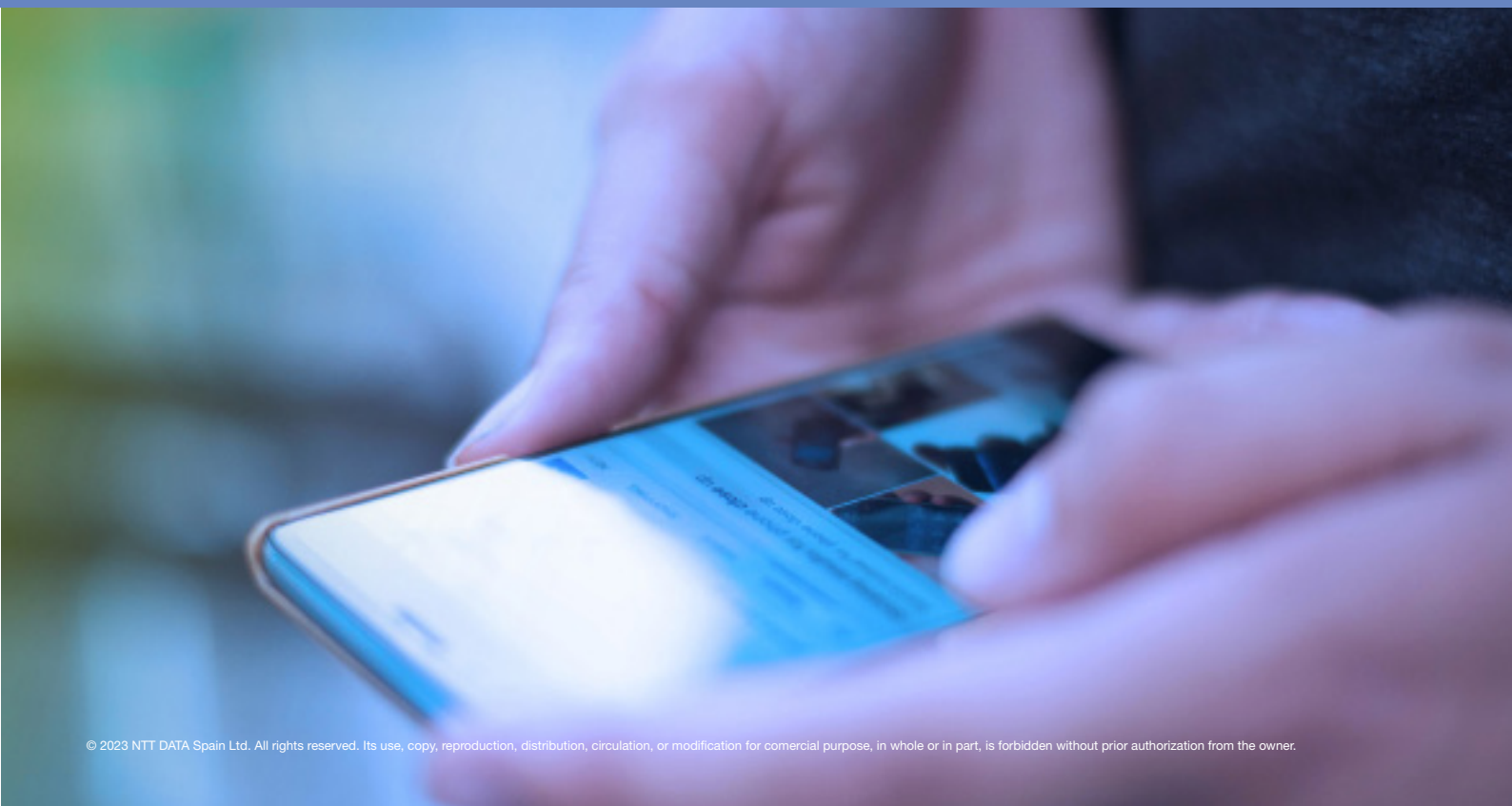
It is a cybersecurity tool that uses artificial intelligence to detect and respond to threats in the digital world. Its purpose is to simplify processes and enhance the capabilities of organisations' security teams. The tool will seek to continuously learn and improve to adapt to the changing threat landscape and enable security teams to be prepared and updated to deal with them effectively.

Link: https://cybersecuritynews.es/microsoft-anuncia-security-copilot-una-solucion-con-ia-para-dar-respuesta-ciberamenazas/

Cigent Secure SSD+

It is an SSD that, thanks to an AI system, has a robust and impenetrable protection against all types of ransomware. Its use could mean the ultimate protection of all files stored within it, which would change everything for organisations, governments, and users.

Link: https://www.adslzone.net/noticias/seguridad/adios-malware-unidad-ssd-ia-evita-infecciones-ransomware/



RESPONSIBLE CYBER

María Pilar Torres Bruna

Cybersecurity Director at NTT DATA Latam and Peru

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

Carla Passos Schwarzer

Cybersecurity Director at NTT DATA Brasil

carla.passosschwarzer@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