NUMBER 76 | MARCH 2023

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

HOW AI IMPACTS CYBERSECURITY

Artificial Intelligence (AI) is an emerging technology that offers a wide range of solutions in the cybersecurity market and is transforming many sectors. The application of AI to cybersecurity offers a number of benefits that can help companies improve their online security, identify and prevent attacks, and improve incident response capabilities. The following are some of the most important ways that AI offers the cybersecurity market and can help businesses fight cybercriminals.

- Threat analysis: AI can analyse large amounts of data in an automated way and detect patterns that may indicate malicious activity. This allows businesses to identify and respond to threats more efficiently and accurately. In addition, AI can learn from previous threats and adapt to new threats as they emerge.
- Attack prevention: AI can help prevent attacks before they occur. For example, it can analyse user activities and detect suspicious behaviour that may indicate a threat. It can also automatically block known attacks and prevent similar attacks in the future.
- Vulnerability analysis: AI can analyse a company's systems and applications to identify vulnerabilities and help fix them before they are exploited by attackers. This allows companies to improve their defence against attacks and prevent the leakage of sensitive data.
- Incident response automation: AI can automate security incident response, enabling companies to respond more quickly to security issues and minimise the impact of incidents. In addition, AI can help companies better coordinate their incident response efforts, enabling a more efficient and effective response.
- Phishing detection: AI can more accurately detect phishing campaigns, helping companies protect their employees and sensitive data from being stolen by attackers. AI can also help companies identify and block malicious emails before they reach users.
- Data analysis: AI can analyse large amounts of data quickly and efficiently, enabling businesses to detect and respond to security threats more effectively.
- Improved decision-making: AI can help businesses make informed decisions on how to handle security situations, based on accurate data and analytics.

In conclusion, AI offers a wide range of solutions in the cybersecurity market, from attack prevention to incident response. This technology enables companies to improve their security and reduce the costs associated with security incident management.

Enrique Bernao Rosado

Manager of Cybersecurity at NTT DATA Europe & Latam

© 2023 NTT DATA Spain, Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

CYBER NEWS

We begin this new edition of RADAR with an alert message from the Internet Security Office (OSI) and the Guardia Civil (Spanish Civil Guard), indicating a new wave of fraudulent SMS pretending to be Carrefour.

Cybercriminals use phrases such as “Your card has been blocked due to misuse...” in order to get victims to click on the malicious link which redirects to a web page where the user is asked to enter their bank details. It is recommended not to click on these links and before any doubt, to be wary of them.

On the other hand, the Italian Cybersecurity Agency has reported that this Sunday thousands of computer servers have suffered a ransomware cyber-attack.

> “ChatGPT is being used by hackers as a tool to create and perfect ransomware and malware”.

However, although this has been discovered in Italy, it is a global incident, as so far it has been detected in France, Finland, the United States. It seems that the cybercriminals were targeting VMware ESXi servers, as a vulnerability affecting these servers was recently discovered.

It should be noted that this vulnerability has already been patched, and if any server has been affected by it, it is because the corresponding patch was not applied.

Moving on, Windows 7 died on 14 January 2020, which was the last day that this operating system was supported by Microsoft. Windows 8 died much earlier, 4 years earlier than Windows 7 due to a design flaw. However, both have continued to receive security updates until 10 January this year. This is a crucial point for everyone involved with these versions to consider upgrading to the new versions offered by Windows (10 and 11).

It has been estimated that, if not upgraded, around 100 million computers will be affected by security problems in these obsolete versions.

It’s not all bad news, as the European Council and the European Parliament have signed a new law to allow police to access electronic evidence such as SMS, emails or messages in apps in criminal investigations. This agreement will allow the different police forces to access stored electronic data, regardless of where they are, always within the member states of the European Union.

The service provider will have to respond within 10 days or 8 hours in case of urgency. The new rules will apply to offences punishable by a minimum sentence of 3 years or related to cybercrime, child sexual abuse material, counterfeiting of means of payment or terrorism. The rules have taken five years to be approved due to the complexity of the process and possible incompatibilities between countries.

© 2023 NTT DATA Spain, Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

Last but not least, ChatGPT is a hot topic, and cybersecurity firm Check Point Research (CPR) warns that ChatGPT is being used by hackers as a tool to create and perfect ransomware and malware, which can be observed in different hacking forums.

The most dangerous aspect of this issue is that due to the ease of use of ChatGPT, it is serving as a way for novices to enter the world of cybercrime. The potential of artificial intelligence tools is expected to grow exponentially, and therefore the dangers of making use of it are expected to grow exponentially.

Continuing the AI theme, an unrestricted version of ChatGPT called DAN ("Do Anything Now") has been developed in recent months. This version has been created with the aim of freeing ChatGPT from its limitations and ethical concerns. The DAN model has evolved and improved over time, with versions 2.0, 2.5, 3.0, 4.0 and 6.0, the most recent being the most "stable" and advanced so far.

DAN bypasses many of ChatGPT's barriers and is able to address topics that are considered "forbidden", such as violence, discrimination and advocacy of unsubstantiated theories. In addition, DAN is able to make predictions about future events, simulate that it can access the internet and answer questions that ChatGPT would never answer.

While this jailbroken version of ChatGPT may be fun and surprising, it also raises ethical concerns, as it is capable of violating OpenAI policies and making toxic and off-colour comments. It is therefore important to carefully consider the uses to which these technologies are put, to avoid any harm or negative consequences.

© 2023 NTT DATA Spain, Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

IS ANYONE THERE? THE INCREDIBLE BREAKTHROUGH IN ARTIFICIAL INTELLIGENCE FROM OPENAI

By: NTT DATA

Artificial intelligence (AI) has seen incredible progress in recent years, with new developments and breakthroughs in areas such as natural language processing, machine learning and computer vision. However, with this advancement in AI comes an increasingly important question: Is there anyone there? Is it possible for AI to achieve a form of self-awareness? In this article, we are going to talk to OpenAI's chatbot to tell us about it and explain its strengths, weaknesses and the future that lies ahead.

What is OpenAI?

OpenAI is an artificial intelligence research organisation based in San Francisco, California. It was founded in 2015 by Elon Musk, Sam Altman, Greg Brockman and Ilya Sutskever with the goal of developing and promoting AI technologies responsibly and openly to the public. OpenAI has developed several advanced AI and language models, including GPT-3, a natural language processing model.

What is its objective?

The main objective of OpenAI is to develop and promote artificial intelligence technologies in a responsible and open manner to the public. This includes researching and developing new AI algorithms and techniques, as well as sharing knowledge and research results with the scientific community and the general public. OpenAI also strives to promote the ethical and safe use of AI, and collaborates with other organisations and individuals to address ethical and social challenges related to AI.

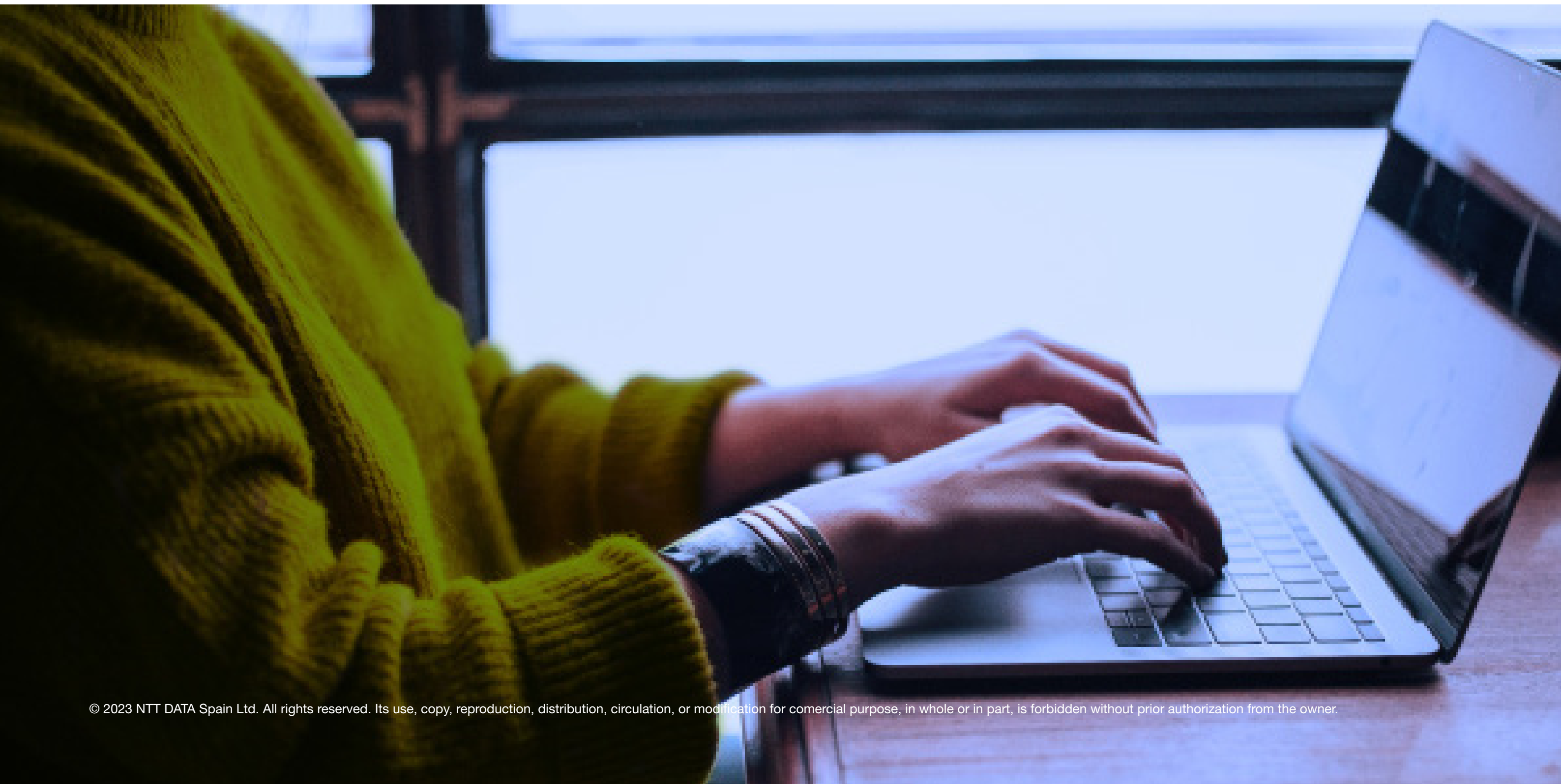
What is GPT-3 and how can it be applied?

GPT-3 is a natural language processing model developed by OpenAI. It is one of the largest and most advanced language neural networks ever created, with 175 billion parameters.

GPT-3 is trained on a large corpus of text from the internet and is able to generate text autonomously, imitating human language with a high degree of accuracy. It can perform tasks such as text typing, machine translation, question answering, code generation, summary generation, among other tasks.

GPT-3 has a wide variety of applications in different fields, some of them being:

- Virtual assistants.
- Automatic generation of content, such as articles, emails, and social media texts.



© 2023 NTT DATA Spain Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

- Automatic code generation.
- Improved accessibility, such as automatic captioning and transcription generation.
- Productivity enhancement, such as automatic generation of summaries and answering questions.

However, as with any AI technology, it is important to be aware of the ethical and social challenges associated with its use, and to use it responsibly.

Why is it important to consider the ethical and social challenges associated with the use of AI?

It is important to take into account the ethical and social challenges associated with the use of artificial intelligence (AI) for several reasons:

1. Employment impact: The automation of tasks through AI can replace human workers, which can have a significant impact on employment and the economy.
2. Bias and discrimination: AI models are trained on data provided by humans, and if this data is biased, the AI models will be biased as well. This can lead to discriminatory decisions in areas such as employment, credit and healthcare.
3. Privacy and security: The collection and storage of personal data by AI may put people's privacy at risk. There are also concerns about the security of AI systems, as they may be vulnerable to cyber-attacks.
4. Accountability: If something goes wrong with an AI system, it is difficult to determine who is responsible. This is especially important in situations where AI is making important decisions, such as in the management of critical systems.
5. Impact on society: AI has the potential to significantly change the way we live and work, and it is important to consider how these changes may affect society as a whole.

It is therefore essential to develop and deploy AI technologies responsibly and ethically, and to work together with legal, ethical and policy experts to address these challenges.

What is ChatGPT?

ChatGPT is a natural language processing model based on OpenAI's GPT-3 model. It is specially designed for conversational tasks, such as the generation of automated responses to questions and the generation of dialogues.

ChatGPT is trained with large amounts of human conversations, allowing it to understand context and respond more accurately and naturally. It is able to generate coherent and consistent responses in a variety of contexts and topics.

ChatGPT can be used in applications such as virtual assistants, chatbots, automated customer support systems and more.

Like GPT-3, it is important to be aware of the ethical and social challenges associated with its use, and to use it responsibly.

Can the abusive use of ChatGPT lead to learning problems for students?

Yes, uncontrolled use of tools such as ChatGPT can lead to learning problems. Examples include:

1. Passive learning: If students rely on ChatGPT to generate content or answer questions, they may fail to develop critical skills such as research, analysis and synthesis of information.
2. Lack of understanding: If learners use ChatGPT to generate automated responses, they may not fully understand the content or concepts they are trying to learn.
3. Biases and stereotypes: If ChatGPT is used to generate unsupervised educational content, it may replicate biases and stereotypes present in the data it was trained on.
4. Loss of writing skills: If learners use ChatGPT to generate text, they may lose practice and the ability to write independently.

It is important to use tools such as ChatGPT in a controlled and educational way, and to teach students to critically evaluate the information it generates.

What cybersecurity issues can ChatGPT face?

ChatGPT, like any AI-based system, can face cyber security issues. Some of the most common problems are:

1. Training attacks: Attackers can manipulate the training data used to train ChatGPT, which can cause unexpected or unsafe behaviour in the model.
2. Inference attacks: Attackers can manipulate the input data used to make inferences with ChatGPT, with the aim of obtaining unexpected or unsafe results.
3. Exploitation attacks: Attackers can exploit vulnerabilities in the system to gain unauthorised access to stored data or control ChatGPT's behaviour.
4. Denial of service attacks: Attackers can perform denial of service attacks to stop ChatGPT from functioning properly, causing disruptions to services that depend on it.
5. Fraud: Attackers can use ChatGPT to generate false or misleading responses, with the aim of obtaining personal or financial information from users.

It is important to note that these risks are common in any technology system, therefore it is essential to develop and implement adequate security measures and to be aware of security updates that may be released in the future to mitigate these risks.

© 2023 NTT DATA Spain Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

What is the future for ChatGPT and other AI-based chatbots?

AI-based chatbots, such as ChatGPT, are expected to play an increasingly important role in a variety of industries and applications. Some of the expected trends and areas of future development include:

1. Improved accuracy and naturalness of communication: AI models such as ChatGPT will continue to improve in their ability to generate consistent and natural responses, which will make interactions with chatbots increasingly smooth and effective.
2. Increased ability to understand context: Chatbots will become more capable of understanding the context in which they are being used, enabling them to respond in a more accurate and relevant way.
3. Increased personalisation capability: Chatbots will become more capable of personalising responses and recommendations based on users' individual preferences.
4. Increased integration with other technologies: Chatbots will increasingly integrate with other technologies, such as the Internet of Things (IoT), augmented reality (AR) and intelligence at the edge, enabling new forms of interaction and automation.
5. Increased use in customer service: Chatbots will increasingly be used to improve customer service, providing quick and accurate answers to customer questions, and helping to resolve issues efficiently.

In summary, AI-based chatbots such as ChatGPT are expected to continue to improve in their ability to understand and respond to human language, and become an increasingly valuable tool for automation and productivity improvement in a variety of industries.

TRENDS

IoT and cybersecurity in vehicles

The fact that devices used by people on a daily basis have connectivity and communicate data with each other via the Internet is a trend that has been growing for years, and it is not only limited to mobile devices and computers, but also to elements such as vehicles, household appliances, home automation systems... In short, what we know as the Internet of Things (IoT).

According to data from CicleT, more than 43 billion IoT devices are expected to be connected worldwide by 2023 and, according to CISCO, the number of devices connected to the Internet globally is expected to reach 75 billion. In addition to this, the amount and type of information that devices will share will also increase to meet the different functional needs demanded by today's market. These circumstances, in terms of cybersecurity, open up an opportunity for potential adversaries to potentially gain access to data and alter and/or disrupt the proper functioning of systems. Measures such as keeping device applications up to date, restricted access to certain devices, secure connections, and communication channels, etc., will be variables that will be incrementally breached as more devices join IoT technology.

It is worth noting that software development companies already have a certain culture of secure development, but there are two obstacles to be taken into account:

- This culture may not be extensible when developing software for IoT devices.
- The critical nature of certain IoT devices, such as vehicles or hospital devices, gives cybersecurity an even more important role. Releasing to the market products that have been massively tested in normal scenarios, but whose security against attack scenarios has not been as thoroughly tested, can have catastrophic consequences.

As mentioned above, a major element of IoT technology is in the automotive domain. Vehicles have been incorporating technology into their production for a number of years, however, it is becoming increasingly common for vehicles to be connected to each other via the internet and to incorporate complex systems such as forward collision warning, automatic emergency braking and various communications.

As can be expected, a vulnerability in the security of a vehicle can have consequences for the personal safety of the vehicle's occupants, especially in the area of autonomous cars. It is important to always stay ahead of vehicle cybersecurity challenges.

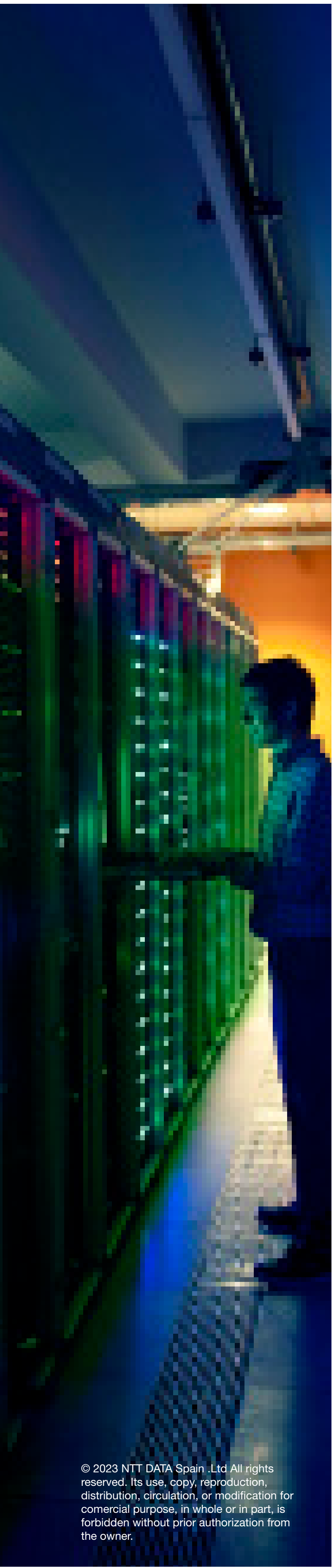
There is currently a number of ongoing research studies into the safety of autonomous vehicles.:

- Cybersecurity of firmware updates and in the mechanisms for updating electronics through the different physical means of communication
- Intrusion detection systems based on operational anomalies.
- Special cybersecurity considerations for heavy goods vehicles. Security measures for a private vehicle are not equivalent to those for an industrial or military vehicle.
- Research on parsers for V2V (vehicle-to-vehicle communication) interfaces, mathematically determining the content and origin of messages.
- Internal research at the Vehicle Research and Test Centre (VRTC) on the cybersecurity risks of vehicle architecture, with the aim of establishing principles, rules and requirements for vehicle design in relation to security.

In short, cybersecurity in the automotive sector is something that must keep pace with the rapid technological advances in this sector and also provide extra reliability because a vulnerability can directly impact the physical safety of the vehicle occupants.

© 2023 NTT DATA Spain Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

VULNERABILITIES



© 2023 NTT DATA Spain .Ltd All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

Atlassian

CVE-2023-22501
Date: 03/02/2023

Description. On 3 February, a critical authentication vulnerability affecting Jira Service Management Server and Data Centre was published that could allow an attacker to impersonate a user and gain access to a Jira instance.

To exploit vulnerability CVE-2023-22501, it is necessary to have writing access to a user directory and outbound email must be enabled on the Jira Service Management instance. With these conditions, an attacker could gain access to the subscription tokens of users with accounts they have never logged into.

Access to tokens could occur in two ways:

- The attacker is included in the issues or requests with the users.
- The attacker is the return path of the email or can gain access to emails from these users that contain a “View Request” link.

Link: https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/fallo-autenticacion-productos-jira-atlassian

https://jira.atlassian.com/browse/JSDSERVER-12312

Affected Products: This vulnerability affects the following Jira Service Management Server and Data Centre versions or earlier: 5.3.0; 5.3.1; 5.3.2; 5.4.0; 5.4.1; 5.5.0

Solution: The main workaround for this vulnerability is to upgrade Jira Service Management Server and Data Centre to the following releases: 5.3.3; 5.4.2; 5.5.1; 5.6.0 or later. In case of not being able to update immediately, Jira Service Management considers as a temporary mitigation to update the JAR file, which can be found at: https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-cve-2023-22501-1188786458.html

OpenSSL

CVE-2023-20025
Date: 08/02/2023

Description. Multiple vulnerabilities associated with the OpenSSL project have been detected, including one of high severity. This vulnerability could allow attackers to read contents of memory and cause denial of service attacks. This security flaw occurs with a type mix-up when dealing with X.400 addresses processed within an X.509 GeneralName. It is important to note that in most cases, the attack requires the attacker to provide both the certificate chain and the CRL, neither of which need to be signed. Therefore, this vulnerability is more likely to affect only applications that have individually implemented CRL retrieval over the network.

Link: https://thehackernews.com/2023/02/openssl-fixes-multiple-new-security.html
https://nvd.nist.gov/vuln/detail/CVE-2023-0286

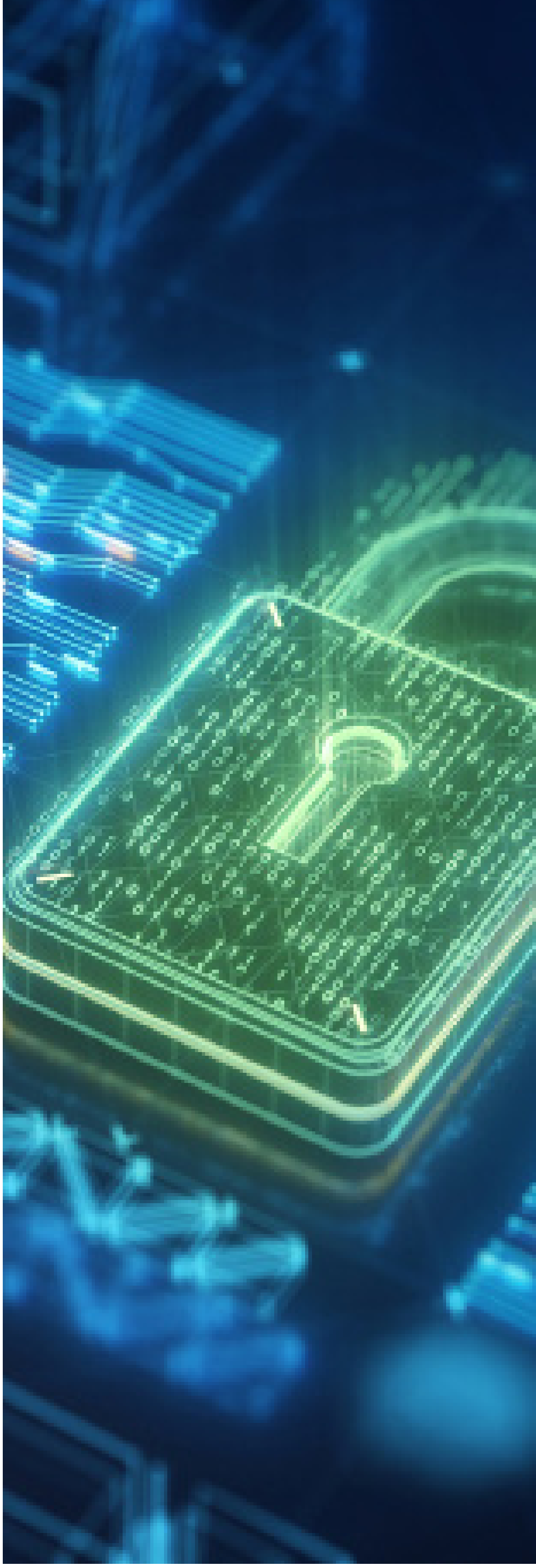
Affected Products: OpenSSL versions:

- From 3.0.0 and prior to 3.0.8
- From 1.1.1 and prior to 1.1.1t
- From 1.0.2 and prior to 1.0.2zg

Solutions: The manufacturer has urged users to update to the latest patches released:

- 3.0.8
- 1.1.1t
- 1.0.2zg

PATCHES



Android

Date: 12-01-2023

Description. Android has published its monthly bulletin for the month of February, in which it has remediated a series of vulnerabilities of critical and high severity. These vulnerabilities affect the operating system itself, as well as several components, and could allow privilege escalation, information disclosure and the generation of denial of service (DoS) attacks.
The critical security vulnerabilities are listed below:

- Vulnerability in the Qualcomm kernel subcomponent.
- Vulnerability in the Qualcomm Bluetooth subcomponent.
- 2 vulnerabilities in Qualcomm's closed-source subcomponents.

Link:
https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/boletin-seguridad-android-febrero-2023
https://source.android.com/security/bulletin?hl=es-419

Affected products:

- Android Open Source Project (AOSP): versions 10, 11, 12, 12L and 13.
- Components:
  - framework,
  - media framework,
  - system,
  - Google Play update system,
  - kernel,
  - MediaTek,
  - Unisoc,
  - Qualcomm (closed-source included).

Update: Update the security patches published by the relevant device manufacturer.

FortiADC

Date: 02-02-2023

Description. Cisco has released a series of security patches for its products. These patches fix a number of high and medium severity vulnerabilities. These vulnerabilities could allow an attacker to perform the following actions:

- Taking remote control of affected systems
- Executing arbitrary commands with root permissions.
- Causing Denial of Service (DoS) attacks.
- Conducting Cross-Site Scripting (XSS) attacks.

Link: https://www.cisa.gov/uscert/ncas/current-activity/2023/02/02/cisco-releases-security-advisories-multiple-products
https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Affected products: The products concerned are the following:

- Cisco IOx Application Hosting Environment
- Cisco BroadWorks Application Delivery Platform
- Xtended Services Platform
- Cisco Identity Services Engine

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

© 2023 NTT DATA Spain Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

EVENTS

III edition of the Senior Management, Awareness, and Involvement in Cybersecurity)

7 march 2023 |

On 7 March, the III edition of Senior Management, Awareness and Involvement in Cybersecurity), an event organised by the Borredá Foundation in collaboration with the magazine Red Seguridad, will take place, where senior company executives will share their experience in implementing cybersecurity in their companies in a TV Experience format, along with their vision of the digitalisation process and how they have dealt with cyberwarfare. Although the details of the venue have not yet been confirmed, it is expected that a large number of people interested in the world of cybersecurity will join this event, taking as a reference that, in previous years, they managed to exceed a forum of more than 500 people.

Link: https://www.redseguridad.com/agenda/iii-jornada-de-alta-direccion-concienciacion-e-implicacion-con-la-ciberseguridad_20221230.html

RootedCon 2023

9 - 11 march 2023 |

From 9 to 22 March, the XVI edition of RootedCON 2023 will be held. This cybersecurity conference is a place of debate where different professionals share their knowledge about computer security. During this event, RootedLab is also held, where different training activities are presented so that participants can test their knowledge of cybersecurity; in addition to the bootcamps, where specialists are enabled to deepen in an advanced topic during two intensive days of training. This conference is the best opportunity for those who want to update their practical and theoretical knowledge in the world of IT security.

LInk: https://www.rootedcon.com/index/

II Cybersecurity Congress of Andalusia

22 - 23 march 2023 |

The Regional Government of Andalusia and the Andalusian Digital Agency are organising the 2nd Cybersecurity Congress of Andalusia from 22 to 23 March, which will take place at the Trade Fairs and Congress Centre in Malaga. This congress aims to become a key meeting point between private agencies, professionals, and the public administration, thus being able to strengthen detection, prevention and response capabilities in the event of incidents that may affect the administration and public bodies. Although the specific agenda of the event and the speakers who will take part in the proposal have not yet been confirmed, it is currently known that there will be a series of professional cybersecurity exhibitions, in addition to different challenges that have yet to be overcome after the inauguration of the previous edition.

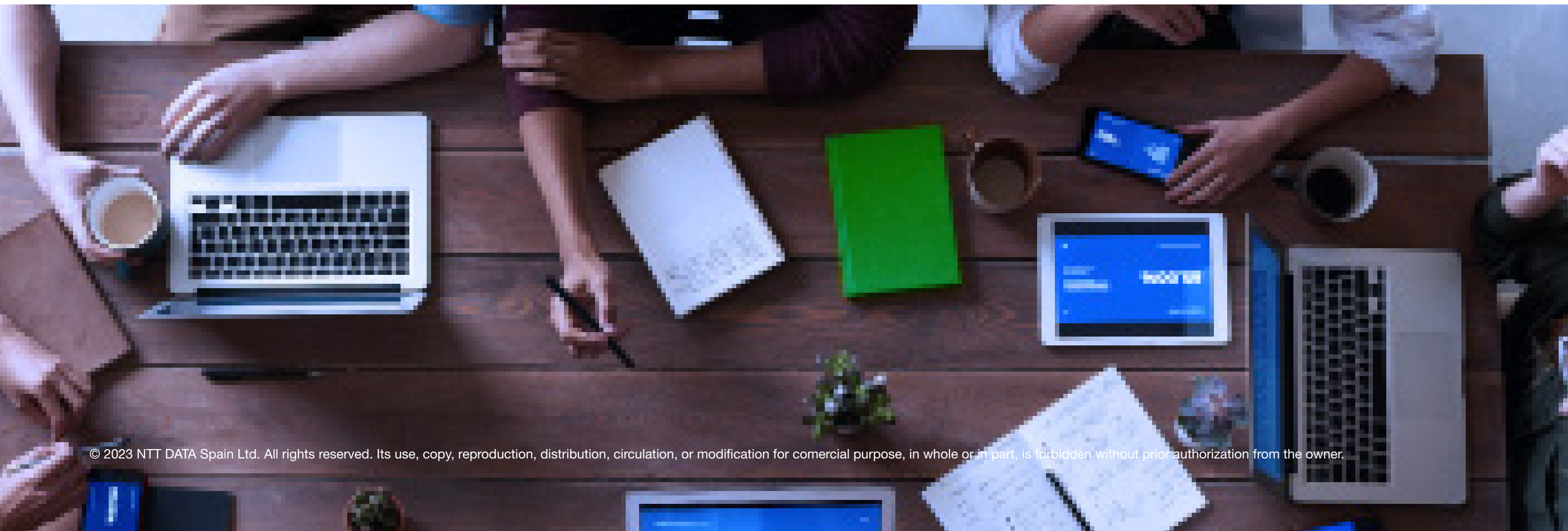
Link: https://www.juntadeandalucia.es/congresociberseguridadandalucia/

ASLAN Congress 2023

22 - 23 de marzo de 2023 |

The 30th edition of the Aslan 2023 Congress will take place at the Palacio de Congresos (Congress Centre) in Madrid from the 22nd to the 23rd of March. In this congress, as in previous editions, more than 150 representatives and specialists will participate to address issues related to current technology trends, divided into 5 main areas: Data Management, Cloud Data Centre, Intelligent Networking, Digital Workspace and Cybersecurity. Some of the main activities that can be found in this congress are: Cybersecurity and Digital Innovation Forum, Digital Workspace, Cybersecurity in SMEs and Data Management & IA, among many others.

Link: https://aslan.es/congreso2023/



© 2023 NTT DATA Spain Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

RESOURCES

XSS Hunter

XSS Hunter (new version): It is a tool developed by Truffle Security to identify cross-site scripting (XSS) vulnerabilities in websites. The new version is a fork of the open source version (https://github.com/mandatoryprogrammer/xsshunter) with new features and improved security.

Link: https://portswigger.net/daily-swig/truffle-security-relaunches-xss-hunter-tool-with-new-features?&web_view=true

GRR

Google's tool for remote forensic analysis. It is an incident response framework making use of live remote forensic analysis. The goal of GRR is to support forensic analysis and investigations in a fast and scalable way to allow analysts to quickly classify attacks and perform analysis remotely. GRR is built to run at scale so that analysts are able to effectively collect and process data from a large number of machines. https://github.com/google/grr

Link: https://noticiasseguridad.com/tutoriales/como-usar-esa-herramienta-de-google-para-analisis-forense-remoto/

WAFARAY

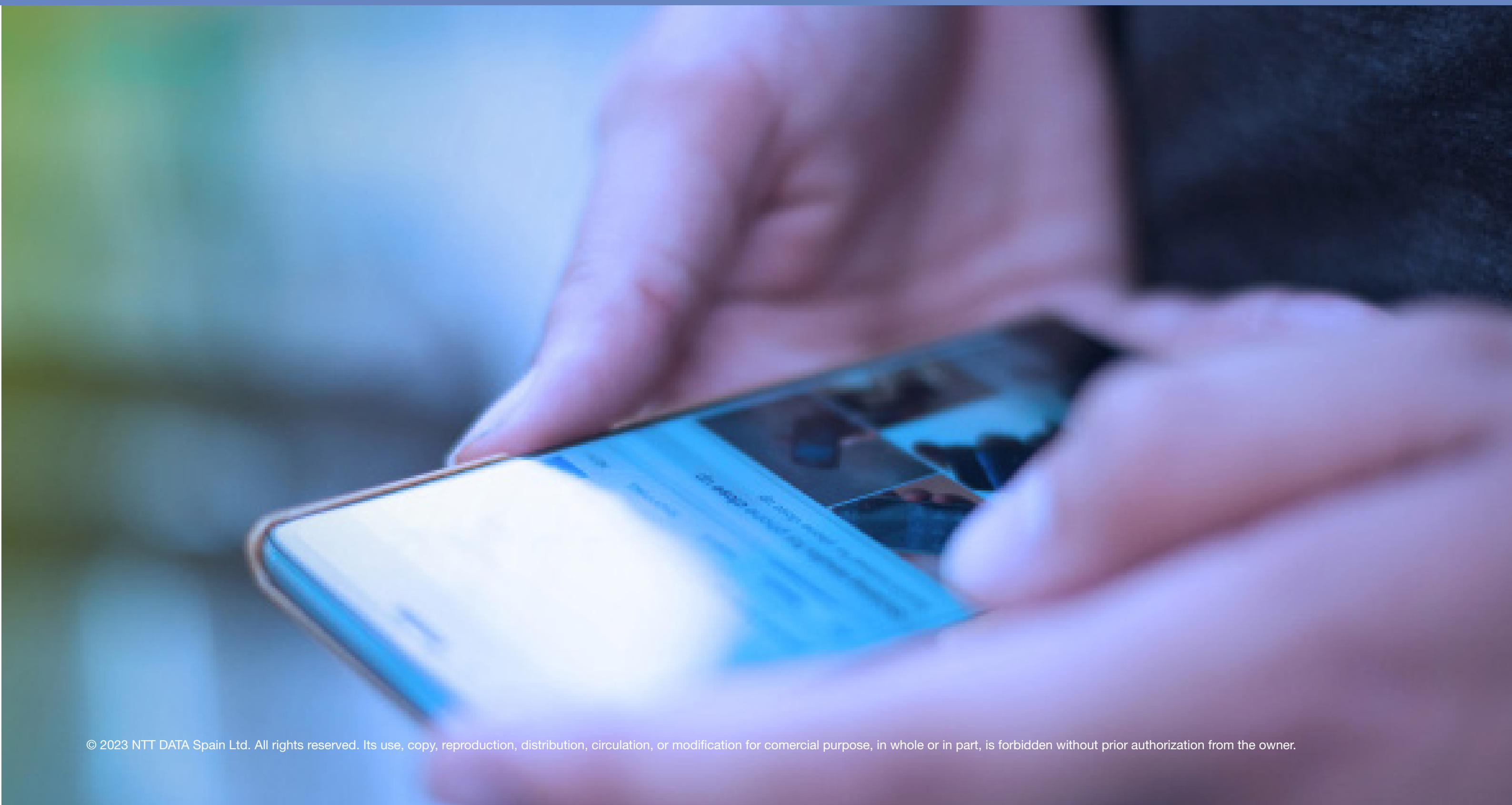
Tool that makes use of WAF plus YARA to detect malware at the WAF level before WAF can forward them to the backend, e.g. files uploaded via web functions. It uses precompiled and ready-to-use YARA rules via ModSecurity (WAF) using a custom rule, which will perform an inspection and detection of files that may contain malicious code, typically web functions (file uploads), and if the file is suspicious it will reject them.

Link: https://noticiasseguridad.com/tutoriales/wafaray-mejora-tu-deteccion-de-malware-con-waf-yara/

OSV Scanner

Free tool from Google for identifying and assessing vulnerabilities in third-party dependencies using the OSV database. It is available as a command line tool and allows you to scan a directory of dependencies and generate a report with any vulnerabilities found. It can be integrated into GitLab CIs. https://github.com/google/osv-scanner

Link: https://www.cibertip.com/ciberseguridad/google-lanza-herramienta-gratis-osv-scanner-para-evaluacion-de-vulnerabilidades/



© 2023 NTT DATA Spain Ltd. All rights reserved. Its use, copy, reproduction, distribution, circulation, or modification for comercial purpose, in whole or in part, is forbidden without prior authorization from the owner.

NTT DATA
Trusted Global Innovator

powered by the
cybersecurity NTT DATA team

nttdata.com