NUMBER 78 | MAY 2023

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

PRIVACY AND SECURITY IMPACT OF 5G NETWORKS

5G is the fifth generation of mobile phone technologies that promises significantly faster data speeds, much lower latency, and network segmentation to be able to provide on-demand services. 5G technologies respond, among other aspects, to the continuous increase in the demand for telecommunications services by private users, companies, and Public Administrations. The traffic and the need are increasing, which puts current networks under great pressure. According to the National 5G Plan, this technology will support the massive increase in devices associated with the Internet of Things, which will increase worldwide from 15,400 million devices in 2015 to 75,400 million in 2025, will provide each terminal with much faster file download times and will be able to serve many more terminals simultaneously, which is known as ultra-dense communications and custom networks (Network slicing).

But associated with all these benefits we also have new security risks, according to the Spanish Data Protection Agency (AEPD), there are three elements of 5G technology that can have an impact on privacy and security: virtualisation, edge computing, and localisation. Undoubtedly, the biggest revolution and what can have the most important impact on privacy is the use of virtualization technologies. Network functions are a set of parameterizable and dynamically creatable virtual components, each with a specific function, which are designed stateless and separating computing functions from data storage functions. Each slice consists of a set of network functions defined in the 5G standard

Edge computing technology will make it possible to shift the ”centre of gravity” of data processing from servers to locations closer to the user’s terminal device, when necessary. In short, there may be a flow of information and/or services between different locations agreed by network operators and service managers, at points close to the end user and within the mobile telephone network of a telecommunications operator, in principle without being on the Internet. By performing computing tasks as close as possible to the end user, 5G will allow for a reduction in communications latency such that it will allow for near-real-time capabilities.

For this, a much more compact access network is needed, with many access points and less distance between them. This higher density will provide the operator and other agents linked to the exploitation of network data, the ability to locate the user terminal with much greater accuracy than it currently has, reaching location resolutions of less than one meter and, unlike previous generations to 5G, including positioning in three dimensions.

These are some of the risks identified by the AEPD :

- Accurate user geolocation: the fact that 5G uses many more base stations and less distance between them makes network-based geolocation much more accurate.
- Profiling and automated decisions: the increase in the amount and categories of data circulating on the network, multiplied by the number of devices that each citizen will have connected through 5G (IoT), will allow reaching a precise individualization of people and the development of services that allow automatic decision-making about people (AI and services in real time).
- Distribution of responsibility between manufacturers, network operators and service providers: a substantial increase in the number of agents that can participate in the processing of personal data is expected with the deployment of 5G networks and with the explosion of new services. This could lead to problems of ambiguity as to the responsibility for the processing of the data, i.e. that the responsibility of each of the parties is diluted.
- Exponential increase in the area of exposure to cyber-attacks: the increase in services, connectivity, interoperability and points of entry and management to the network will increase the opportunities for threats to privacy to materialize.
- Dynamism in communications management functions: if in previous generations the network management functions were, in fact, wired, the possibility of updating it through software introduces problems of stability, version traceability, updates by various actors, backdoors, factory malware and hacking.
- Possible loss of user control: this may occur on data flows, with possible cross-border implications, as well as on the exercise of rights. 5G uses a distributed and dynamic processing model, where it is planned that data and processing will be moved in real time to the physical location where they are most needed or their processing is most effective

Therefore, in order to extract the maximum advantages from technology and reduce its possible risks, we need more than ever a digital rights framework, and a clear net neutrality environment since, for example, the fact that the infrastructure that supports networks is going to be based on software has many advantages, but also disadvantages, and that is that it may have greater risks of attack and espionage. On the other hand, 5G networks should be considered critical infrastructures and, therefore, especially protected.

José Arturo Cueto Marín

Solutions Project Leader at NTT DATA Colombia

CYBER NEWS

This month's cyber chronicle begins with the Fortinet FortiGuard Labs report that has identified critical security vulnerabilities in Cacti, Realtek and IBM Aspera Faspex, which are being exploited by various malicious actors to attack unpatched systems. Among the vulnerabilities, CVE-2022-46169 and CVE-2021-35394 stand out, which are being used to distribute botnets such as MooBot and ShellBot.

The first, a variant of Mirai, has been used for the first time, while the second has been detected in three different versions: PowerBots (C) GohacK, Light's Modded perlbot v2 and B0tchZ 0.2a. In addition, all three have the ability to carry out distributed denial of service (DDoS) attacks, as well as perform file uploads and downloads and run a reverse shell.

> "OpenAI's announcement, which has revealed a bug in the open-source Redis library that has been responsible for exposing personal information and conversation titles of users of its ChatGPT service".

Fortinet researchers have highlighted that compromised systems can be controlled and used as DDoS bots after receiving a command from the C2 server. Therefore, it is important that administrators use strong passwords and change them periodically to prevent such attacks.

We continue with OpenAI's announcement, which has revealed a bug in the open-source Redis library that has been responsible for exposing personal information and conversation titles of users of its ChatGPT service.

The issue was detected on March 20, 2023, and allowed certain users to be able to see the short descriptions of other users' conversations in the chat history sidebar. As a result, the company decided to temporarily shut down the chatbot.

The error originated in the redis-py library, which caused cancelled requests to corrupt connections and return unexpected data from the database cache, in this case, information belonging to another unrelated user.

To make matters worse, OpenAI introduced a change to the server by mistake, which caused an increase in request cancellations, thereby increasing the error rate.

Although the issue has been fixed, OpenAI has acknowledged that the issue could have had more serious implications elsewhere, potentially revealing information related to the payments of 1.2% of ChatGPT Plus subscribers on March 20 between 1 and 10 a.m. PT. The exposed information included first and last name, email address, payment address, the last four digits of a credit card and the expiration date of the same, although the full numbers of the cards were not exposed. The company has contacted the affected users to notify them about the unintentional leak and has added redundant checks to ensure that the data returned by its Redis cache matches the user requesting it.

Finally, SentinelLabs has reported on a hacking tool called “AlienFox”, which is being used to extract sensitive information from misconfigured servers. This tool is a kind of adaptable toolkit that can be modified to meet the needs of attackers. The latest version of the tool extracts sensitive information such as API keys and secrets from configuration files of service providers such as AWS, Google Workspace, Office365, OneSignal, Twilio, Zoho and others.

The AlienFox toolkit is mainly distributed via Telegram and the scripts are available on open source repositories such as GitHub. This has led to a constant adaptation and variation of the tool in nature.

Threat actors use this set of tools to collect lists of misconfigured hosts from security scanning platforms such as LeakIX and SecurityTrails. These misconfigured server configurations are associated with popular web frameworks such as Laravel, Drupal, Joomla, Magento, OpenCart, PrestaShop and WordPress.

Once a vulnerable server is found, the threat actor gains access to files that store sensitive information, such as the enabled services and the associated API keys and secrets.

Researchers have discovered two versions of the tools, starting with version 2 in February 2022. Other researchers identified several scripts as belonging to the Androxgh0st and GreenBot malware families.

Version 2, among the oldest AlienFox tools, mainly focuses on extracting credentials from configuration files or web server environment. The researchers said they analysed the file containing the output when an actor executed the tools, which included access keys and AWS secrets.

The version 3.x of the AlienFox toolkit contains the “cryptocurrency mining agent” script that uses a variety of tools to install malicious software that uses a server’s CPU to mine cryptocurrencies such as Monero. This version also includes scripts to extract credentials from databases and gain reverse shell access.

The emergence of these hacking tools underscores the need for organisations to regularly update and patch their systems and applications to protect themselves from potential vulnerabilities and attacks. In addition, users and organisations should make sure to use strong passwords and change them periodically to prevent unauthorised access.

Finally, we conclude by commenting on the awareness campaign launched by the Ministry of the Interior of Spain that aims to educate citizens about the threats of cybercrime and provide practical tips on how to increase online security. Computer crimes in Spain have increased by 72%, according to data from the Ministry of the Interior, and the campaign seeks to reduce these crime levels. The campaign is being carried out on social networks, using hashtags such as #Cybersecurity and #Safetyonline, and is expected to reach a wide audience. In addition, posters and brochures have been created to be distributed in public places, such as libraries, community centres and schools. The regulation has also been raised as a response to cybercrime, and an explanatory video about cryptocurrency scams has been prepared as part of the campaign.

METADATA AND INFORMATION LEAKAGE

By: NTT DATA

The use of metadata is becoming more and more important nowadays, particularly in the field of computing, due to the amount of information that is handled every day. Metadata is defined as data that describes other data, e.g., metadata for a file can give more information about the file if it includes the author, size, creation, and last modification dates. In terms of storage options, you can choose to use the file itself as a container or make use of an external resource.

Their functionalities include interoperability, facilitating their understanding by both users and machines. Additionally, they facilitate digital identification, since a set of them can act as an identifying and differential set of an object or resource. The latter, if not properly treated and protected, can become a problem of information leakage.

Often, without being aware of it, users generate metadata along with the creation of content, such as a file or a photo. An image taken by a digital camera or mobile device may contain a variety of metadata, such as dimensions, camera used or focal length, which are automatically generated after capture and are known as EXIF.

This type of automatic metadata can lead to the exposure of information, such as location, which can be used to geolocate a specific moment in space and time, potentially compromising the user who took it at the time.

In relation to the latter, in 2012 a cybercriminal named Higinio O. Ochoa, known as w0rmer, was arrested thanks to the metadata exposed in a photograph of his girlfriend, which he posted on his Twitter account as a taunt after managing to obtain private data from US agents and police forces. The FBI was able to analyse the metadata in the image and obtain the geolocation of the image, which allowed them to locate the couple's Melbourne flat where the photograph was taken. Subsequently, with the help of his girlfriend's Facebook profile, they identified Ochoa as his partner and therefore the person hiding behind the pseudonym w0rmer. In addition, his arrest was confirmed after corroborating the IMEI of his mobile phone, which was also exposed in the metadata of the image.

Another even older case is that of a serial killer named Dennis Rader, known as the BTK Killer. He began his crimes in 1974 and it was not until more than 30 years later that he was finally caught.

As in the previous case, he taunted and teased the police about their inability to arrest him, so much so that he even sent a final letter in 2005, which contained a floppy disk with a file on it, thinking that it would still be impossible to trace him. The police found a .doc file that had previously been deleted from the floppy disk, which contained some metadata, such as the last user who modified the file (Dennis) and the software licence that belonged to a Lutheran church. After a search of this information and a DNA comparison they managed to catch him after many years of searching.

Both cases reveal the importance of metadata and how it can expose information that can work against those who generate such files or images. It is therefore important to analyse what impact they may have within the field of cybersecurity.

Metadata is particularly relevant when it comes to OSINT (Open Source Intelligence). OSINT is a technique for gathering information from open sources that is accessible to everyone, with the aim of gathering valuable information about a target. That is why, in this context, metadata can play an important role in gathering information about organisations, people or events.

Applications of metadata in the OSINT field include:

- **Geolocation:** Many cameras and mobile phones now include in the metadata information about the geographical location where a photograph was taken or a video was recorded. This can be useful for determining a person's location, studying their movements, or identifying relevant places.
- **Document analysis:** Digital documents may include information about the author or the date of creation, among others. In this case, metadata is used to facilitate document classification, distribution, storage, and control.
- **Email research:** Email headers include metadata, among which we can find information about the sender, recipients, or date of sending. The information contained in them can help protect against spam or phishing.
- **Trend analysis:** Website metadata can include information about how often a site is accessed or the geographic location of users, which can be useful to identify trends and patterns of behaviour.

These are just a few examples, as metadata can be useful in other contexts and applications. In general, metadata is a valuable tool in OSINT, as it can provide a more complete understanding of the target being studied.

However, it is important to keep in mind that metadata can also be manipulated or falsified, so it is essential to verify the authenticity of the information before using it.

As seen above, metadata is a great source of valuable information. However, it can also have a detrimental effect on the privacy and security of information. At the user level metadata often impacts more negatively than positively, especially when information is shared online. As seen in the known case examples, metadata stores relevant information that can put the user's privacy at risk. Some of the metadata that stand out as privacy threatening are geographic location information, personal information (names, e-mail addresses, etc.), camera data in the case of audio-visual resources or dates of creation or modification. To avoid this, certain measures can be taken, such as deleting metadata using deletion tools or editing it manually, disabling automatic collection in most programs such as Microsoft Office or Google Drive, or using applications that do not store this type of information.

On the other hand, when talking at the enterprise level, it is usually necessary to maintain such metadata, as it helps in the organisation and classification of information or data analysis. Therefore, it is essential to protect them properly by following a series of good practices for their management, some of which include:

- **Access control:** Limiting access to authorised persons and systems.
- **Encryption:** Encrypting sensitive metadata to protect it from theft.
- **Secure storage:** Storing it in secure systems to help restrict unauthorised access.
- **Updating:** Keeping security systems up to date.
- **Policies and procedures:** Establishing clear policies and procedures for the use and protection of metadata.
- **Education and awareness:** Raising users' awareness of the importance of protecting metadata and enabling them to follow good metadata management practices.
- **Deletion of metadata:** Deleting metadata when it is no longer needed by using metadata deletion tools..

In general, metadata security is essential to ensure the privacy and integrity of information. By following good metadata management practices, risks can be minimised. However, it should be noted that this is not a complete solution for information security and privacy, and additional measures need to be taken to achieve this.

RELIABLE MANAGEMENT OF CLOUD COMPUTING

By: NTT DATA

Cloud computing is currently a necessary and critical environment for the processing of information by technology. We can say that this environment meets or can successfully meet the vast majority of services and applications of all organisations. However, However, to be in the Cloud does not automatically mean to be involved in Cloud Computing and to meet the criteria for proper Information Security Management, Cybersecurity and Privacy Protection. There are security criteria for proper management.

The CSA - Cloud Security Alliance, a global entity of professionals and independent providers of services and products, initially defined the Security Guide for the Critical Areas of Focus in Cloud Computing, and later improved for ENISA - European Union Agency For Cybersecurity publishing the Benefits, Risks and Recommendations for Information Security in Cloud Computing. The CSA considers 13 Domains of Controls that should be implemented for Information Security Management, Cybersecurity and Privacy Protection of Trust for the Cloud Computing Environment.

1. Domain of Architecture

Defines the standards and frameworks (NIST, ISO, etc.) that must be taken into account to apply the solution.

2. Governance and risk management

Cloud services and products must be evaluated based on risks and aligned with governance: technological, security and corporate.

3. Legal requirements, contracts and other obligations.

It is necessary to take into account the applicable legislation, the regulations of regulatory bodies and other obligations that the organisation must comply with.

4. Audit

The information management solution in the cloud must be auditable. The level of requirement and the granularity of the type of audit will depend on the type of company, the size, the location in the country and other controls. The organisation must be aware of what needs to be taken into account.

5. Information governance

It defines the processing of information, the responsibilities and competencies that the different agents have in relation to the processing of information.

6. Continuity of the environment for business continuity.

Defines the best guarantee controls so that the environment remains available in case of unavailability of the cloud service provider. This control must be well defined and formalised in a contract. The degree of continuity of the service provider should also be defined.

7. Security infrastructure

The cloud service must and should guarantee an excellent security infrastructure, so that the service provided is in a reliable environment. This degree of efficiency of the infrastructure must be explicit and contractual.

8. Virtualisation and containers

Virtualisation is one of the strong features of cloud computing. However, it is necessary to define or identify who (Provider or Contracting Organisation) is responsible for Virtualisation and its security controls. In addition, some of these controls are provided by the provider, but they must be implemented by the organisation.

9. Response to incidents

Cloud computing must also take into account that incidents (more or less serious) occur and the provider must have a communication and accountability structure. The virtual environment can facilitate certain controls, but it cannot fail to consider Incident Management, including tests to ensure its effectiveness.

10. Application security

The application does not change whether it runs in the cloud or traditionally on local servers. It is necessary to define well how the security controls will be managed and whose responsibility it is. Another issue is the applications that are already generated in the cloud environment. They have different characteristics than traditional applications and their security specificities must also be taken into account.

11. Data security and cryptography

Definition and control is necessary for the data need to use encryption. Depending on the organisation and the type of company, some data will necessarily have to be encrypted. Once defined how this encryption will be, it is necessary to define and formalise the responsibility for key management and other controls.

12. Identity and access management

This should be one of the first controls to keep in mind when using cloud computing. It usually remains the sole responsibility of the organisation. Even if a cloud service is contracted, access management is the responsibility of the organisation. The provider can and should facilitate this control.

13. Security as a Service

Security as a Service (SaaS) allows an organisation to protect its information resources in the cloud by contracting a service from the provider. It is undoubtedly an excellent option, considering that the cloud environment has specific characteristics and knowledge, which many organisations and their professionals do not have. However, the number of security controls is very wide and must be agreed with the organisation.

14. Related Technologies

The use of Cloud Computing is usually related to the use of other technologies such as Big Data, Internet of Things (IoT), Mobile Services, Operational Technology (OT) and others. It is necessary to validate if what Cloud Computing offers is consistent with the needs of these technologies and use in the Organisation.

All these dimensions make it mandatory for the Organisation to carry out a Due Diligence about the cloud service you intend to hire or have already hired.

Conclusion

Cloud computing can have numerous advantages and a greater ease for there to be security controls. However, it does not happen by magic. It is necessary to consider all the dimensions presented by the CSA - Cloud Security Alliance. Of course, this is not the only reference, but it is an entity unrelated to providers and provides guidelines and guidance for organisations.

TRENDS

AI extensions, the new market for cybercriminals.

Security in web browsing is an issue of vital importance nowadays, as more and more people make use of the internet and the different tools found on the web. One of the main risks in this area are browser extensions, which can be a source of problems in terms of security and privacy.

Installing extensions in web browsers may seem like a simple and harmless task, but in reality it can cause many problems if the necessary precautions are not taken. One of the main causes of these problems is the lack of information about the author of the extension and its functions. In this way, cybercriminals generate this type of software with malicious intentions, inserting malware that can put the security of our computer or our personal information at risk.

In addition, many extensions have the ability to access the user's personal information, such as browsing history, passwords stored in the browser, geographic location, among others. Another risk related to browser extensions is the presence of spyware and key loggers. These programmes can monitor and log the user's online activities, including passwords and other sensitive information. If a user installs an extension with these features, he or she could become a victim of identity theft or other types of fraud.

Booming AI as a focus

A concrete example of the risks that can be presented by installing browser extensions is the creation of malware extensions that are associated with the use of ChatGPT. ChatGPT is an artificial intelligence tool that allows you to interact with an automated chat system to get answers to specific questions. If a malicious developer creates a browser extension that pretends to be a ChatGPT extension, it could trick users into downloading and installing it on their browsers, allowing them to access their personal information and put their security at risk.

To avoid these problems, it is important for users to always make sure to download and install browser extensions from trusted sources and to research the reputation of the developer before installing any extensions. In addition, it is important to carefully read the privacy policies and terms and conditions of extensions before installing them in the browser.

In conclusion, the installation of extensions in web browsers can be a source of problems in terms of security and privacy if the necessary precautions are not taken. It is important for users to always be aware of the risks involved in installing an extension and to inform themselves about the developer and the extension's functions before installing it. In this way, they will be able to protect their personal information and their online security.

VULNERABILITIES

VM2

CVE-2023-29017
Date: 08/03/2023

Description. On 6 April, KAIST WSP Lab researchers discovered a critical vulnerability in the VM2 library, a JavaScript sandbox used to safely execute untrusted code in a virtualised environment. The vulnerability is detailed below:

- CVE-2023-29017: This vulnerability could allow an attacker to bypass sandbox protections and remotely execute code on the host. This is due to an error in the handling of host objects passed to the 'Error.prepareStackTrace' function when an asynchronous error occurs.

Following the release of the version that addresses this vulnerability, two variants of a PoC have been published for the exploitation of this vulnerability.

Link: https://github.com/advisories/GHSA-7jxr-cg7f-gpgv
https://gist.github.com/seongil-wi/2a44e082001b959bfe304b62121fb76d
https://thehackernews.com/2023/04/researchers-discover-critical-remote.html

Affected products. The vulnerability affects version 3.9.14 and earlier of the VM2 library.

Solución: The main solution is to apply the security patch released on 7 April corresponding to VM2 version 3.9.15.

Apple

CVE-2023-28205, CVE-2023-28206
Date: 07/04/2023

Description. On 7 April Apple released an emergency security patch to address two actively exploited 0-day vulnerabilities. Both are of high severity and are detailed below:

- CVE-2023-28205: This vulnerability affects the WebKit framework used by the browsers of all iPhones and iPads, including Safari, as well as any application that uses this framework in the rendering process. This vulnerability could allow arbitrary code execution after accessing a malicious website.
- CVE-2023-28206: This vulnerability affects the Apple's IOSurfaceAccelerator framework and could allow arbitrary code execution with kernel by a malicious application.

In the statement published by Apple, they report the active exploitation of these vulnerabilities. Using the first vulnerability, CVE-2023-28205, an attacker could gain control of the browser used by the user and run a malicious application that exploits the second vulnerability, CVE-2023-28206, which could result in control of the device.

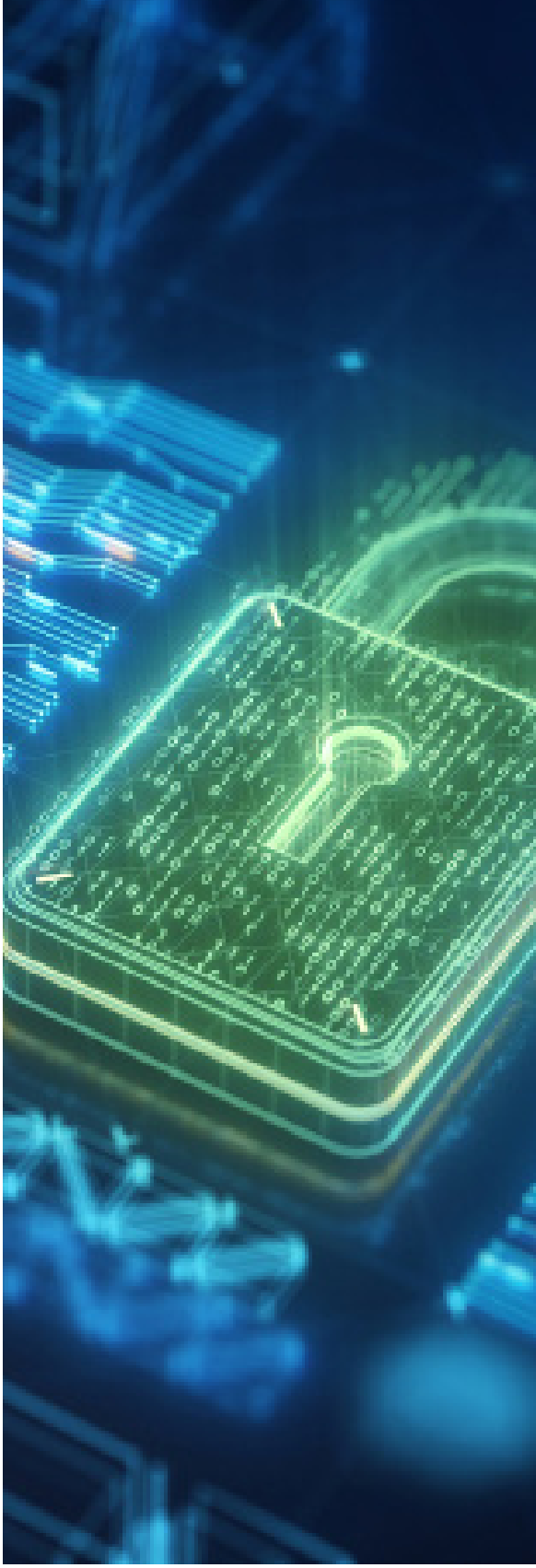
Link: https://support.apple.com/es-es/HT213720
https://support.apple.com/en-us/HT213721
https://support.apple.com/en-us/HT213722
https://support.apple.com/en-us/HT213723
https://support.apple.com/es-es/HT213724
https://support.apple.com/es-es/HT213725
https://news.sophos.com/es-es/2023/04/10/apple-publica-parches-de-emergencia-para-exploits-dia-cero-de-tipo-spyware-actualiza-ya/#:~:text=CVE%2D2023%2D28206%3A%20un,propio%20n%C3%BAcleo%20del%20sistema%20operativo

Affected products

These vulnerabilities affect the following Apple products: iOS prior to version 16.4.1; iPadOS prior to version 16.4.1; macOS Ventura prior to version 13.3.1;macOS Monterey prior to version 12.6.5; macOS Big Sur prior to version 11.7.6; Safari prior to version 16.4.1

Solution: The main solution to solve these vulnerabilities is to apply the corresponding security patch, that is, to update the systems to the following versions: iOS to version 16.4.1;iPadOS to version 16.4.1; macOS Ventura to version 13.3.1; macOS Monterey 12.6.5; macOS Big Sur 11.7.6; Safari to version 16.4.1

PATCHES



Android

Date: 03-04-2023

Description. Android has published its monthly bulletin for the month of April, which includes 2 security patches. These patches remediate a number of vulnerabilities of critical, high, and moderate severity. These vulnerabilities affect the operating system itself, as well as several components, and could allow privilege escalation, information disclosure, the generation of denial of service (DoS) attacks or remote code execution.
The critical security vulnerabilities are detailed below:

- Two vulnerabilities, CVE-2023-21085 and CVE-2023-21096, which affect the system component and could allow remote code execution by an attacker without requiring execution privileges or user interaction.
- Four vulnerabilities, CVE-2022-33231, CVE-2022-33288, CVE-2022-33289 and CVE-2022-33302, which affect the Qualcomm closed-source component and could lead to memory corruption.

Link:
https://source.android.com/docs/security/bulletin/2023-04-01?hl=es-419
https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/boletin-seguridad-android-abril-2023

Affected products:

- Android Open Source Project (AOSP): versions 11, 12, 12L and 13.
- Components: framework; system; Google Play update system; kernel; Arm; Imagination Technologies; MediaTek; UNISOC: Qualcomm (including closed-source).

Update: Update the security patches published by the manufacturer of the affected components.

Cisco

Date: 05-04-2023

Description. Cisco has released updates to its software on 5 April to address two vulnerabilities categorised as high criticality. Successful exploitation of either of these vulnerabilities would allow an attacker to escape the restricted shell and gain root privileges, due to incorrect validation of parameters sent to a specially crafted CLI command. However, both vulnerabilities require the attacker to be an authenticated local user:

- CVE-2023-20122: for this vulnerability, the authenticated user can be an administrator account or an account with the “read-only” permission.
- CVE-2023-20121: In Cisco EPNM and Cisco Prime Infrastructure, the attacker needs an administrator account to gain root privileges to exploit this vulnerability but can still exploit the vulnerability. However, in Cisco ISE, the vulnerability can only be exploited through an administrator role.

No active exploitation of either vulnerability is identified.

Link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk
https://www.securityweek.com/cisco-patches-code-and-command-execution-vulnerabilities-in-several-products/

Affected products: Some of the affected products are as follows: Cisco Evolved Programmable Network Manager (EPNM) version 7.0.0 or earlier; Cisco Identity Services Engine (ISE) version 3.2; Cisco Prime Infrastructure version 3.10 or earlier

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

EVENTS

Hack-Én

May 5 - 7 2023 |

The first edition of Hack-Én will be held from 5 to 7 May. This national cybersecurity conference will be held in Linares, Jaén where the latest trends and solutions in information technology will be addressed. This congress provides a highly professional atmosphere for speakers and attendees, offering the unique opportunity to establish valuable relationships with leading sponsoring companies in the industry. Among the activities available at the event, attendees will have the opportunity to participate in keynote lectures and interactive sessions. In addition, there will be practical workshops and live demonstrations so that attendees can put their knowledge into practice and learn in a practical way.

Link: https://hack-en.org/

Cyber Security Summit – OpenExpo

May 13 2023 |

On 13 May, the Cybersecurity Summit will be held at OpenExpo Europe, one of the largest professional trade fairs on Business Technology Innovation in Europe. Every year, experts gather at the Cybersecurity Summit to discuss the latest trends, challenges, and solutions in the field of cybersecurity, especially related to enterprise cybersecurity. From common threats such as phishing and malware to industry-specific vulnerabilities, such as risk in cloud environments and data protection. Attendees also have the opportunity to learn about new security tools and solutions being developed to address these challenges.

Link: https://openexpoeurope.com/es/cybersecurity-summit-2023/

Cybersecurity Expo

May 23 2023 |

The second edition of the Cybersecurity Expo will take place on 23 May, bringing together IT security managers, CISOs, CIOs and CIOs in a highly relevant professional meeting. During this exclusive event, leading experts will share their knowledge and cutting-edge practices in Cybersecurity, with the aim of controlling the risks and threats posed by cyber-attacks. This meeting will be an excellent opportunity to learn first-hand about cybersecurity trends and share experiences with other professionals in the sector.

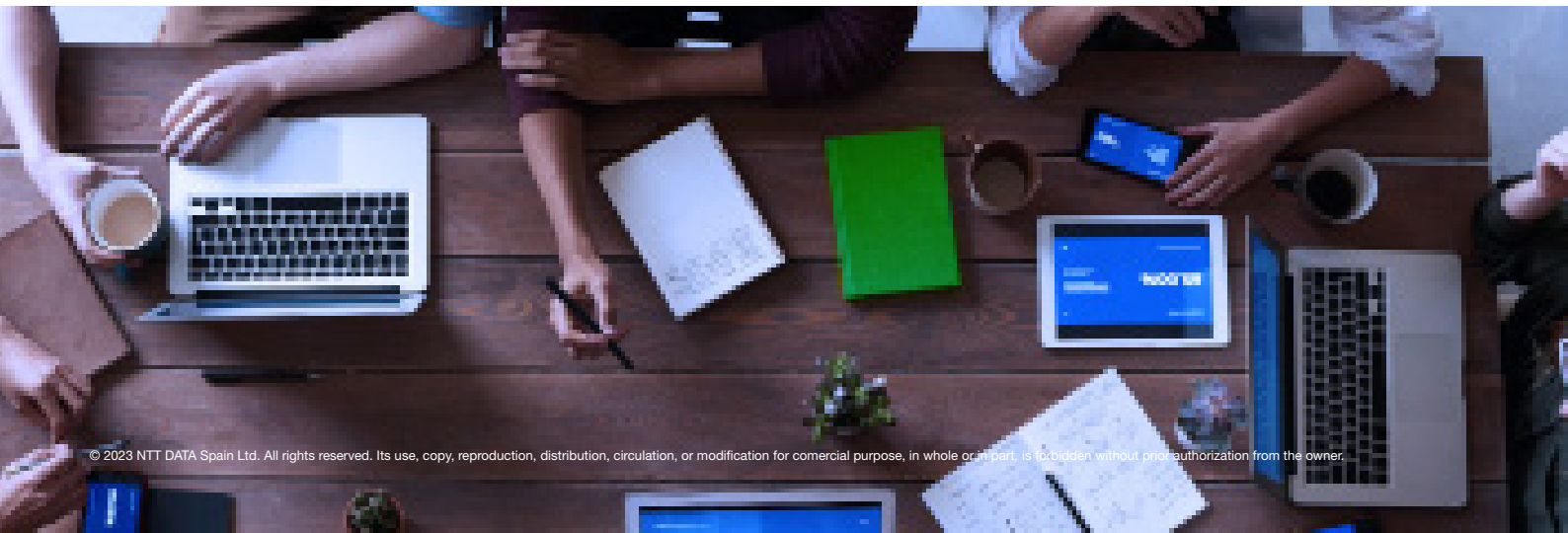
Link: https://ciberexpo.ifaes.com/

Security Forum

May 31 - June 1 2023 |

SANS Pen Test Austin 2023 is six days of in-depth, hands-on training in penetration testing, network teaming, purple teaming and exploit development for professionals who need to know how to find vulnerabilities within their organisations, understand risk and prioritise resources based on potential real-world attacks.

Link: https://plataformadenegocio.es/securityforum



RESOURCES

ZincSearch

ZincSearch is a search engine that performs full-text indexing. It is a lightweight alternative to Elasticsearch and runs using a fraction of the resources. It is used as an underlying indexing library. It is very simple and easy to operate, unlike Elasticsearch, which requires a dozen configurations to understand and fine tune. It is a direct replacement of Elasticsearch if you are only deploying data using API and searching using Kibana. ZincSearch is a lightweight alternative to Elasticsearch that requires minimal resources, written in Go. Although Elasticsearch is a very good product, it is complex and requires a lot of resources. Zinc makes it easier for people to use full text search indexing without making much effort.

Link: https://github.com/zinclabs/zincsearch

TruffleHog

The TruffleHog tool is a security tool developed by a community that is passionate about security. It is used to detect API keys, passwords and secrets that have been compromised to Git. This tool is capable of locating high entropy keys on GitHub to protect the networks and sensitive data of administrators. In addition, TruffleHog is also an open source Chrome browser extension that searches for API keys and credentials on visited websites and alerts you if any are present. The tool can also be used for penetration testing and code reviews to identify keys that would otherwise be lost or would have to be searched manually. TruffleHog is also available as a package on operating systems such as Kali Linux and can be installed via pip install [7, 8]. The tool can be customized with additional regular expressions and rules can be added with a specific flag.

Link: https://github.com/trufflesecurity/trufflehog https://trufflesecurity.com/trufflehog/

Trivy

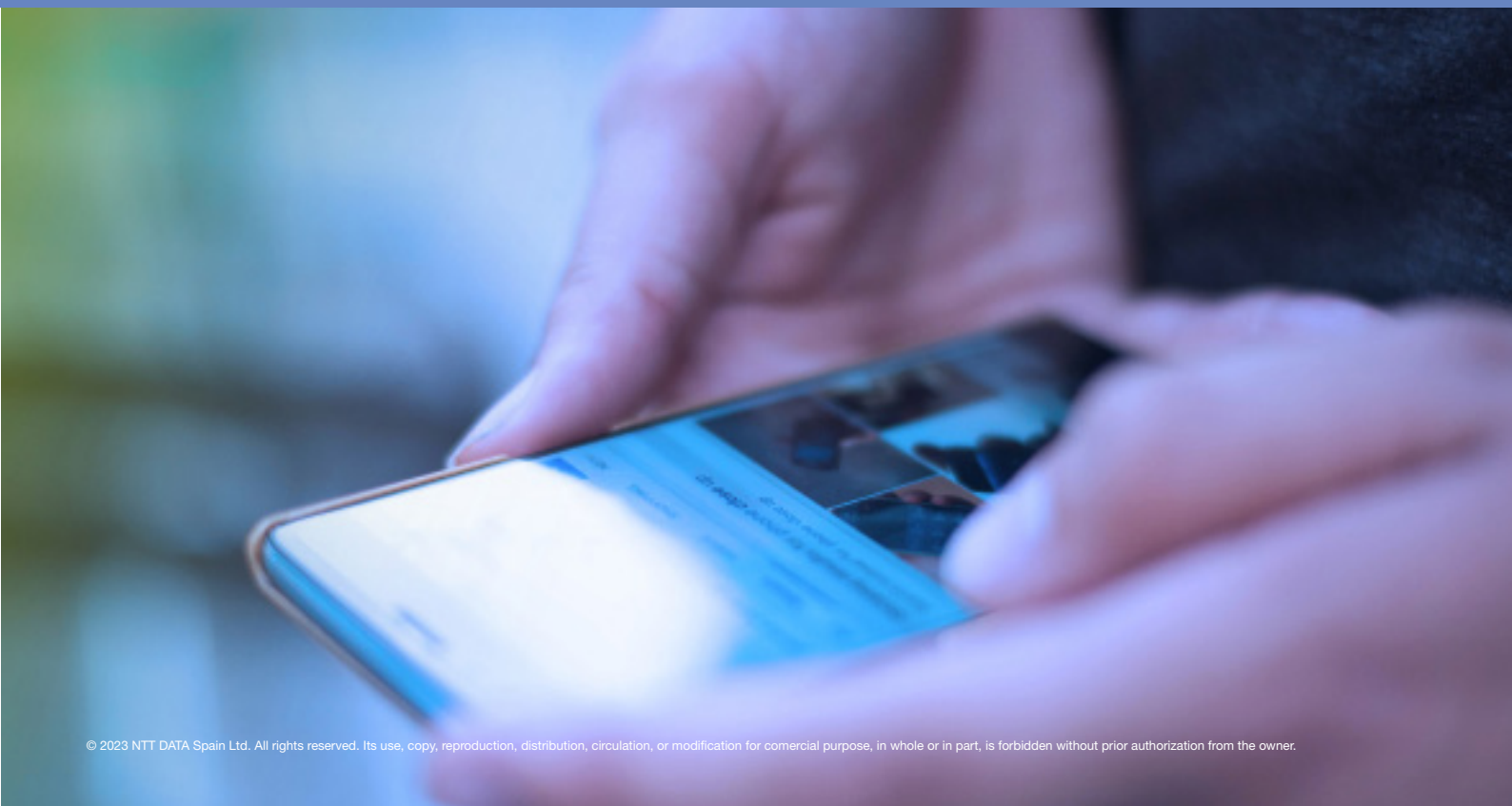
Trivy is a versatile and complete security scanner, designed to detect security issues and vulnerabilities in different environments, such as containers, Kubernetes, code repositories, clouds and more. Trivy can also find confidential information and secrets, as well as problems and misconfigurations in the management of infrastructure as code. With Trivy, greater security can be guaranteed on the network of the desired platform.

Link: https://github.com/aquasecurity/trivy

Wazuh

Wazuh is an open source host-based intrusion detection (HID) system. It is an evolution of the OSSEC software, which is its direct precursor and has additional functions such as automatic log analysis. The Wazuh platform offers monitoring, detection and alert of security events and incidents. It is capable of protecting workloads in on-premises, virtualized, containerized and cloud environments and is used for threat prevention, detection, and response. Wazuh is a complete tool derived directly from the OSSEC repositories, which provides full network support, complies with security regulations, and has several additional management functions. It is an open source, enterprise-ready software that helps to identify threats, monitor integrity, give rapid responses to incidents, and maintain compliance.

Link: https://github.com/wazuh/wazuh https://www.azulweb.net/wazuh-la-plataforma-de-seguridad-de-codigo-abierto/



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