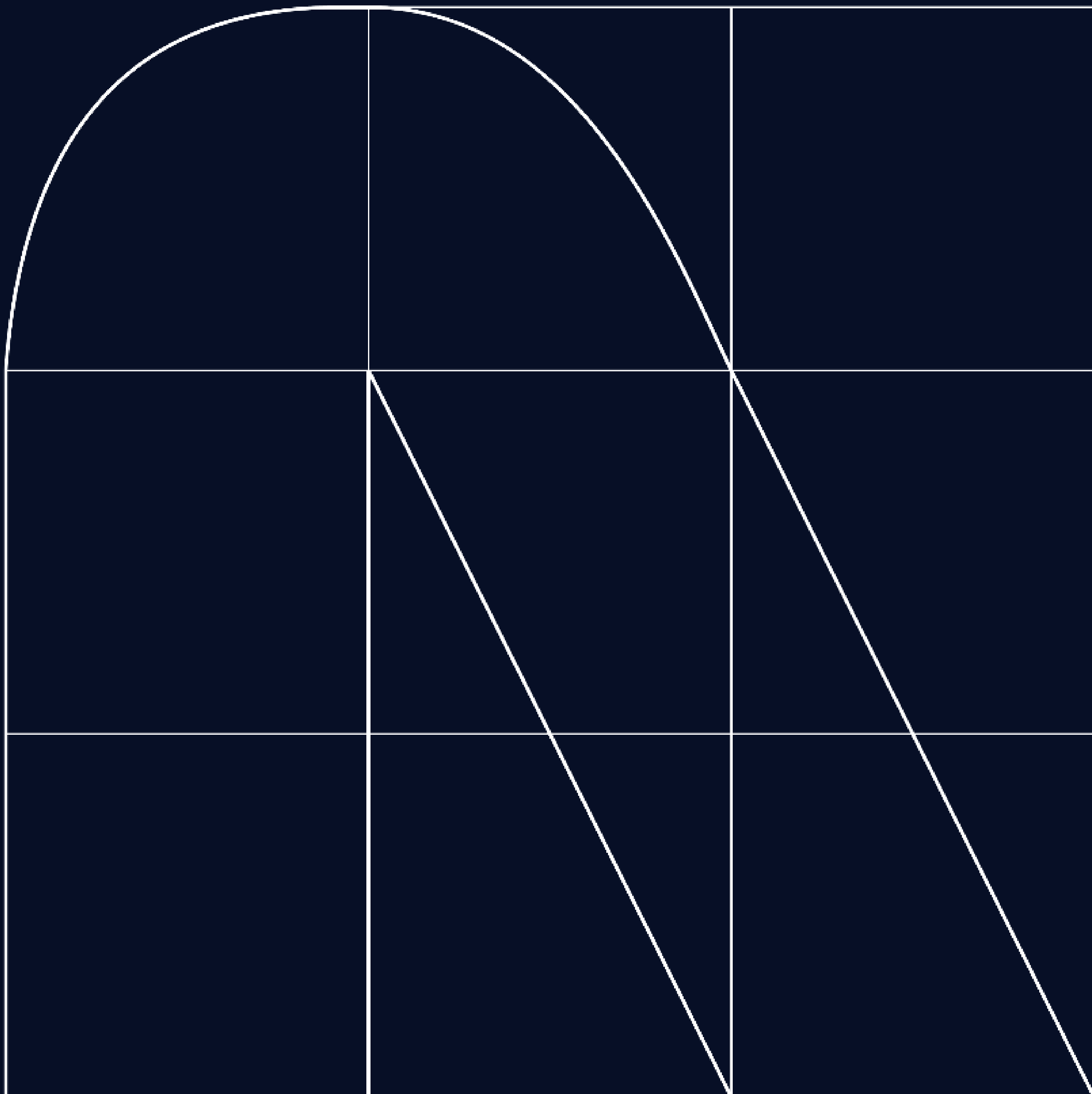
Number 84 | November 2023

NTT DATA

Radar

Cybersecurity magazine



Submarine communication cables, a critical infrastructure that needs protection.

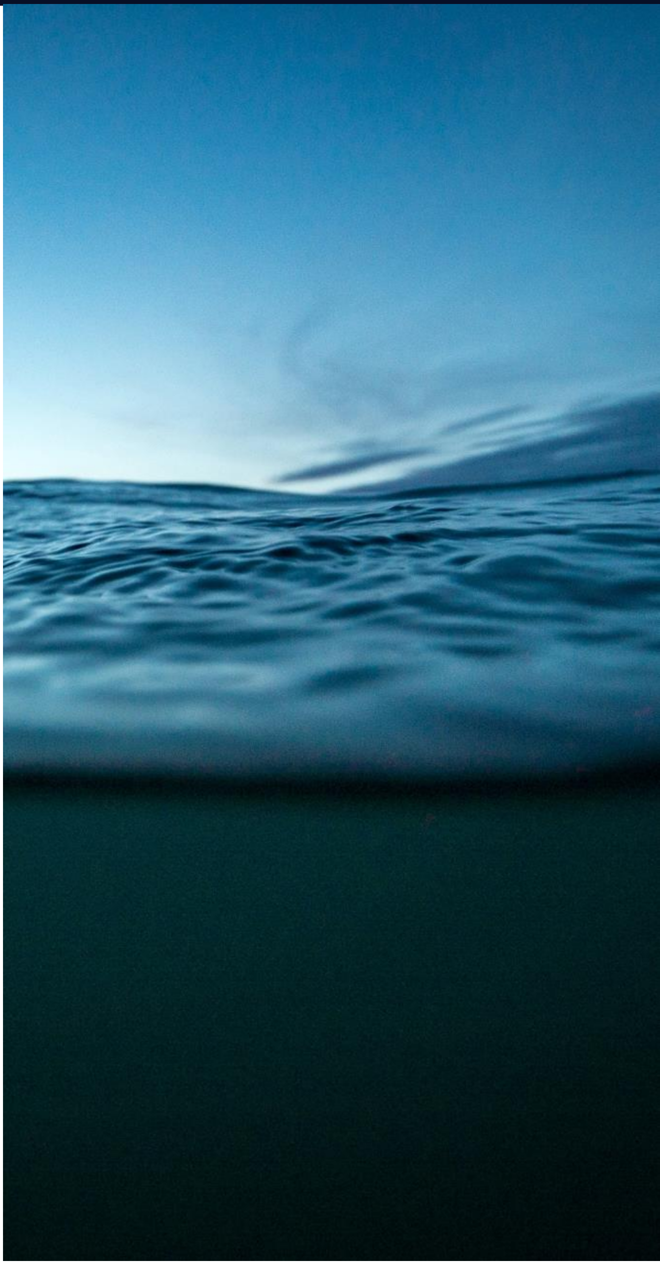
By: Mª Ángeles Gutierrez

Global communication relies heavily on a critical infrastructure that often goes unnoticed: undersea communication cables.

These cables, which stretch for thousands of miles on the ocean floor, are the backbone of global connectivity, enabling the transmission of data, voice, and video across oceans. However, and although the exact location of these networks is kept secret and encryption techniques are used to protect information, the growing reliance on these underwater networks – 99% of the world's digital communications transit the network – has increased concern about the cybersecurity risks they face. Cable security has been a little-studied element in international security (according to a report by the European Parliament "Security threats to undersea communications cables and infrastructure – consequences for the EU" June 2022), and it is not at all simple, as it affects ocean governance, digital sovereignty, critical infrastructure policy and various aspects of external action, from defence policy to security policy.

There are about 400 cables in the world, of which 250 pass through Europe, Spain connects 4 continents with 32 landing points: Europe, Africa, Asia and North America and is the strategic global connection point of the European Union.

The annual average of incidents that cause outages is approximately one hundred. The vast majority are caused by negligence in fishing operations near them, but the accumulation of outages in recent months has once again raised the possibility of other types of attacks or sabotage, increasing the alert about this type of infrastructure, which has motivated the latest ENISA report, "SUBSEA CABLES - WHAT IS AT STAKE?" published at the end of July this year. This document points out that almost 40% of cable failures are due to anchoring or fishing, while in almost the other half there is no specific cause. In total, 87% of incidents are caused by human intervention, either unintentional errors or intentional malicious actions, only 4% of incidents are attributed to system failures and 5% are due to natural phenomena.



Artificial intelligences (AIs), such as ChatGPT, are not necessarily designed specifically for cybersecurity, but they can be trained to perform tasks related to computer security.

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 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 in identifying patterns and anomalies, it can be applied to various cybersecurity tasks, such as intrusion detection, identifying malware, monitoring network activity, predicting malicious behaviour, and automatic response to security events.

To maintain effective cybersecurity AI, 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 needed to ensure accuracy and effectiveness in protecting computer 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 media, with the goal of learning patterns and associations in natural language. Through this ongoing training, the model becomes increasingly accurate and effective in its ability to understand and generate natural language.

In short, submarine communication cables are a critical part of the global telecommunications infrastructure that enables long-distance communication around the world. Its security and reliability are of paramount importance for today's global economy and society, cybersecurity risks are a growing concern in an increasingly interconnected world and on which according to the European Parliament's report not enough focus has been placed until now. Protecting this critical infrastructure is essential to guarantee the security and continuity of our global communications, which is why we propose that the threats related to this issue be added to the risk analyses and that in addition to an exhaustive follow-up and monitoring of their evolution be carried out to detect and alert as soon as possible.

María Ángeles Gutierrez
Cybersecurity Manager at NTT DATA Europe & Latam

Cyberchronicles

By: NTT DATA Europe & Latam

Artificial intelligence has become a very powerful tool for both large-scale attacks and cyber defences.

In recent conflicts, we have seen how cyber warfare tactics have been used to gain strategic advantages. These cyberattacks include system infiltration, disinformation, and disruption of online services.

Artificial intelligence (AI) has been a key tool in these cyber attacks, as it allows automation and optimisation of operations. Here are some examples of AI usage for cyber attacks:

Advanced Phishing Attacks: AI is used to create highly personalised and convincing phishing emails, designed to trick recipients to obtain sensitive information.

> “
>
> Cyber warfare in these conflicts is a reminder of how technology and artificial intelligence are being used on the modern battlefield.

Smart Malware: Cybercriminals employ AI to develop malware capable of evading traditional defenses and adapting to real-time conditions.

Vulnerability Detection: Attackers can use AI to constantly look for vulnerabilities in computer systems and networks, allowing them to identify and exploit weaknesses.

Denial-of-service attacks(DDoS): AI is used to coordinate and amplify DDoS attacks, making them more difficult to mitigate.

Disinformation and manipulation on social media: AI can automate the creation and dissemination of fake news and disinformation on social media platforms, which can influence public opinion.

In these cases, artificial intelligence is also used to strengthen their cyber defenses. AI is used to detect threats, identify anomalous patterns, and improve the security of critical systems.

Cyber warfare in these conflicts is a reminder of how technology and artificial intelligence are being used on the modern battlefield. These developments pose significant challenges for cybersecurity and highlight the importance of international cooperation in preventing and mitigating cyber attacks in times of conflict.

FraudGPT

Speaking of other topics, in the last radar we talked about some new tools on the market, such as "FraudGPT". These tools implement AI technology for fraud detection and prevention, and many Spanish companies have already begun to rely on them.

Studies carried out in our country show that fraud continues to be one of the biggest concerns for both companies and consumers. One in five Spaniards admits to having been a victim of fraud in one of their payments, with the average amount of money swindled being around $160. Another of these studies highlights that fraud attempts have been increasing over recent years. Even so, 60% of retailers are confident that their fraud detection systems are effective, with only 24% of them stating that they have invested in prevention and response systems in the last year.

To combat this growing threat, AI is being implemented in fraud detection tools. According to surveys conducted, 53% of Spanish retailers are already harnessing the capabilities of artificial intelligence to defend themselves against fraud, in addition to chargeback management software for cost management and reduction. Considering the current situation and future forecasts, it is recommended that companies invest not only in management and prevention tools but also in customising these to their specific needs, leveraging machine learning, and working on distinguishing legitimate buyers from other malicious actors.

Blockchain resilience: Is a disaster recovery plan necessary?

ANALYSIS

One of the major challenges for companies is to be prepared for a disruption that could jeopardise the continuity of their critical processes, with recovery responses aimed at mitigating the negative impacts generated (reputational, economic, operational, legal, etc.) or potentially generated by the contingency.

The current global context (extreme environmental effects, energy shortages, political tensions, increased cybercrime, etc.) highlights the risk that companies face in experiencing some form of disruption. Organisations are becoming increasingly aware and focusing their efforts on identifying risks that could affect their operations to develop a strategy to mitigate those risks that could endanger the availability of the company's technological services.

One of the most common and recurring strategies for companies is Disaster Recovery Plans (DRPs). These plans are an essential part of any business's operational and security strategy, as they are designed to ensure rapid recovery of operations in the event of unexpected disruptions, whether they are natural disasters or caused by human factors. However, with the emergence of blockchain technology and the decision of some businesses to build their models based on this technology or even migrate their existing models to this new technology, there is a potential shift in practices concerning DRPs.

One of the key features of Blockchain networks is their ability to withstand failures. This quality is derived from their design, which is composed of independent nodes formed by decentralised and distributed networks. Unlike traditional centralised systems, where a failure can paralyse the entire system, Blockchain systems are fundamentally resilient to such interruptions. In a company whose systems are based on Blockchain, such as decentralised applications (dApps) that operate on a Blockchain network, the concept of distribution plays a crucial role in disaster planning. For a Blockchain network to fall, all its constituent nodes must fall, as each node contains a complete copy of the Blockchain and can operate independently.

Ethereum, one of the largest and most popular Blockchain networks in the business world due to its ability to store so-called "Smart Contracts" (self-executing programs stored on a Blockchain network that activate when predefined conditions are met), has several thousand nodes distributed around the world. To force the collapse of this Blockchain network, compromising its nodes would be necessary through one of the following methods:

- For a worldwide natural phenomenon to occur that would devastate all nodes, this event would need to affect all geographical areas with nodes and compromise the electrical supply or internet connectivity, both of which are essential factors for the Blockchain network. Such a phenomenon would result in a service outage for the Blockchain network due to the absence of operational nodes capable of sustaining the network.

- The network could also be compromised through an attack that seeks to take control of the Blockchain network, depending on the network's consensus mechanism. While this may not necessarily affect the service's availability, it would compromise the reliability of the data, as a malicious actor with sufficient control over the network could attempt to manipulate transactions or even reverse previously executed ones, undermining the inherent trust in the system. While it might be relatively easy to compromise a single node (e.g., physically taking control of the node), compromising the entire network would require gaining control over a large number of nodes (51% of the nodes in a Proof of Work system or nodes that collectively hold 51% of the tokens in a Proof of Stake system). This would be an extremely costly process and would almost certainly be identified by the community, who could then take measures to prevent it.

It should be noted that both cases, both the global natural disaster and the massive attack on the nodes, are hypothesised with a very low probability.

It is worth noting that in the realm of security, the three dimensions of security are often discussed: availability, integrity, and confidentiality. Availability ensures access to information when needed, integrity protects information against unwanted alterations, and confidentiality ensures that access is granted only to authorised individuals. Taking these dimensions into account, we can see that the basic features of Blockchain protect availability through the distribution of nodes and ensure the integrity of information as each node contains a cryptographically protected copy of the Blockchain (to guarantee its immutability). Confidentiality, however, is a more significant challenge due to the inherent transparency of Blockchain networks (though there are alternative measures to ensure confidentiality, but they often come with greater complexity).

Therefore, companies that place particular importance on availability and the integrity of information should consider the possibility of incorporating Blockchain into their operations or transitioning their model to this technology.

María Lezana Juberías
Cybersecurity Expert NTT DATA Europe & Latam

Óscar Marimon Rius
Cybersecurity Consultant NTT DATA Europe & Latam

The worrying sophistication of vishing with Generative Artificial Intelligence.

TRENDS

Phishing and its various mutations continue to be one of the most used strategies by cybercriminals today. Despite increasing efforts by companies to educate their employees about these attacks, we still witness numerous examples of this technique in action.

During this year, we have witnessed phishing campaigns that impersonate respected institutions such as the Tax Agency and the Directorate General of Traffic (DGT), using mass fraudulent SMS messages that claim non-existent monetary fines and direct users to malicious websites.

In particular, in recent months, vishing techniques have gained notoriety. Vishing is a type of social engineering phone scam in which the identity of a trusted company, organisation, or individual is impersonated through a phone call in order to obtain personal and sensitive information from the victim. An example of this is a campaign that impersonated the National Cybersecurity Institute of Spain (INCIBE) with the aim of stealing personal data from users. This scheme combined vishing and phishing, starting with phone calls in which attackers posed as INCIBE representatives, attempting to persuade users to provide information, including their email addresses, as part of their fraudulent scheme.

Another notable incident is the hack of MGM Resorts International, a conglomerate that manages some of the largest casinos in Las Vegas. The group of attackers, known as "Scattered Spider," researched MGM employees on LinkedIn and used the identity of one of them to call technical support and request a password reset. In just 10 minutes, the cybercriminals had gained access to the network.

The use of voice and images of individuals for fraudulent purposes is not new, but what's surprising is how easily attackers can manipulate these technologies for their own purposes. Throughout this year, we've seen multiple scam campaigns that employ the voice and image of celebrities, such as Elon Musk, who has been a frequent target of these deceptions, especially in the cryptocurrency space. Some of the most notorious attacks involve hacking YouTube channels with a large audience that suddenly start spreading fraudulent content.

Recently, a fake campaign went viral, using the identity of Jimmy Donaldson, known as MrBeast, to supposedly give away an iPhone 15 Pro to 10,000 people. What's striking about these campaigns is how quickly a cybercriminal can execute them using tools like HeyGen.

When this technology is in the hands of malicious actors with greater knowledge and resources, it can be used to influence international conflicts. An example was seen in Russia, where radio stations and television channels were hacked to broadcast deepfakes of Vladimir Putin, announcing false information about withdrawals and massive mobilisations.

Vishing, when combined with generative artificial intelligence tools, has rapidly evolved and become a significant threat. These attacks exploit identity impersonation, the use of public figures, and voice manipulation to deceive victims. The ease of creating deepfakes and fraudulent campaigns presents additional challenges for cybersecurity.

In response to these challenges, the European Union took the initiative in the middle of this year to push for the first European law on artificial intelligence, expected to be finalised by the end of the year. This law regulates various aspects of AI usage, including systems like ChatGPT. Under this law, providers will be required to identify and mitigate potential risks and comply with transparency requirements by indicating which content has been generated by AI, as well as helping to distinguish real images from "Deepfakes."

Indeed, as a response to the proliferation of AI-generated content, more tools for detecting such content have emerged. Twitter has already launched tools to combat misinformation on its platform, and Google introduced SynthID, a tool specifically focused on detecting AI-generated images.

Beyond personal security implications, vishing can be used to influence international conflicts by spreading false information. This underscores the need to remain vigilant and adopt robust security measures to protect against these ever-evolving threats. Education on scam identification and the implementation of strong cybersecurity measures are crucial in a world where voice and image manipulation technology is within the reach of cybercriminals.

Vulnerabilities

Read our full patches and vulnerabilities newsletter by subscribing here.

Critical Vulnerability in Cisco Emergency Responder

Date: October 4, 2023
Severity: **CRITICAL**
CVE: CVE-2023-20101

Description:

On October 4th, Cisco disclosed a critical vulnerability in the Cisco Emergency Responder application. This vulnerability stems from the existence of static credentials for the root user that cannot be altered or removed. These credentials are typically intended for use during development.

Exploiting this vulnerability could allow an unauthenticated remote attacker to log in to the affected device with the root user, thereby enabling the execution of commands with elevated privileges.

Cisco's Protocol Security Incident Response Team (PSIRT) reports that no public disclosures of this vulnerability have been found.

Link

Affected products:

This vulnerability only affects Cisco Emergency Responder version 12.5(1)SU4.

Solution:

The recommended solution to address this vulnerability is to update the vulnerable installations; the first fixed version being version 12.5(1)SU5.

Vulnerability in Google Chrome

Date: October 3, 2023
Severity: **HIGH**
CVE: CVE-2023-5346

Description:

On Tuesday, September 3rd, Chrome released an update for the desktop application of Google Chrome. This update reports the correction of a high-severity vulnerability. This vulnerability could potentially allow an attacker to perform remote code execution by exploiting memory corruption in the browser's execution stack when using a specially crafted HTML page.

The vulnerability arises from an issue in Google Chrome's JavaScript engine (V8) because it misinterprets data types.

Other browsers like Microsoft Edge, which are based on Chromium, have also been affected by this vulnerability, and Microsoft has already released a security update for it.

Link
Link

Affected products:

The resources affected by this vulnerability are as follows:

Google Chrome, versions prior to version 117.0.5938.149.

Microsoft Edge, versions prior to version 117.0.2045.55.

Solution:

The recommended solution is to update Google Chrome to version 117.0.5938.149 and Microsoft Edge to version 117.0.2045.55.

Patches

Monthly Android Security Bulletin

Date: October 2, 2023
Severity: **CRITICAL**

Description:

On 2 October, Android published its security bulletin for the month of October. The bulletin reports a total of 51 vulnerabilities, including 5 critical vulnerabilities and 46 high vulnerabilities.

Among the critical vulnerabilities are the following:

CVE-2023-40129 and CVE-2023-4863: These are two critical vulnerabilities that could allow an attacker to perform remote code execution. Both vulnerabilities affect the “system” component.

CVE-2023-24855: This critical vulnerability is caused by memory corruption in the modem during the security configuration process prior to AS Security Exchange.

CVE-2023-28540: This vulnerability is caused by improper authentication during the Link TLS protocol causing cryptographic issues in the data modem.

CVE-2023-33028: This is a vulnerability due to memory corruption in the WLAN firmware during the process of making a memory copy of the pmk cache.

The last three vulnerabilities affect the closed-source Qualcomm component.

Link

Affected Products:

The vulnerabilities fixed in this bulletin affect the following resources:
Android Open Source Project (AOSP) versions 11, 12, 12L, and 13.
Components: framework, system, Google Play Update System, Arm, MediaTek
Qualcomm (including closed-source)

Update:

Update affected devices with security patches released by the manufacturer.

Update for a 0-day vulnerability in Apple

Date: October 4, 2023
Severity: **HIGH**

Description:

Apple has released a security update for iOS and iPadOS that fixes a zero-day vulnerability CVE-2023-42824.

The vulnerability identified as CVE-2023-42824 affects the kernel and could grant a local attacker the ability to increase their privilege levels on affected devices. Apple reports that this security flaw may have been used against vulnerable iOS versions.

This security update also covers the CVE-2023-5217 vulnerability, a zero-day security flaw in Google Chrome on September 28. This vulnerability originates due to a stack buffer overflow in vp8 encoding, which is located in libvpx, a video codec library jointly developed by Google and the Alliance for Open Media (AOMedia). This issue was resolved by updating to libvpx 1.13.1.

Link
Link

Affected products:

The vulnerability affects all versions prior to version 16.6. Specifically, it affects the following products:

iPhone XS and later
iPad Pro-12.9-inch, second generation and later
iPad Pro-10.5-inch
iPad Pro-11-inch, first generation and later
iPad Air, third generation and later
iPad sixth generation and later
iPad mini fifth generation and later

Solution:

iOS 17.0.3 and iPadOS 17.0.3

Events

Black Hat MEA

14-16 November

The edition of Black Hat MEA (Middle East and Africa) will be held in Riyadh, Saudi Arabia, from November 14 to 16. This leading event in the region will promote the exchange of knowledge and the dissemination of new technologies through conferences and workshops given by industry experts.

Link

National Cyber League Spain

25 October – 16 November

The National Cyber League is a competition organised in Spain by the *Guardia Civil* (National Spanish Police) that takes place from October 22 to November 16. This competition aims to enhance the talent of young people through a multidisciplinary perspective, addressing technical, legal and communication aspects.

Link

Cyber Security & Cloud Expo

30 November – 1 December

Cyber Security & Cloud Expo is an event that takes place in London from November 30 to December 1, where various topics are addressed, such as artificial intelligence, blockchain and the Internet of Things (IoT), focused on multiple sectors, including cybersecurity.

Link

Resources

New methods of social engineering using AI

Today, artificial intelligence is capable of giving you the ability to assume the identity of another person in real time. This is achieved through applications such as VoiceX, which allows you to modify your voice, and DeepfakeVFX, which allows you to convincingly alter your face. Thanks to these technologies, it is possible to impersonate someone and thus obtain information that can be used maliciously.

Link

The RNS shares more than 30 daily alerts on active cyber threats

The National Operations Network (*Red Nacional de Operaciones* - RNS), under the leadership of the National Cryptologic Centre (*Centro Criptológico Nacional* - CCN), reports more than 30 ongoing cyberthreats daily, providing participating entities with the opportunity to take action to mitigate potential risks.

Link

Raspberry Pi5

At the end of October, the Raspberry Pi 5 will be available for sale, a single-board computer with substantially improved performance compared to its predecessor. This technological advancement will allow IT enthusiasts and professionals to pursue a wide range of projects with greater efficiency and versatility.

Link

HelloKitty ransomware leak

On 9 October 2023, the HelloKitty ransomware was leaked on a hacking forum, which has caused significant problems for companies such as CD Projekt in 2021 and Cloudflare in 2022. As a result of this leak, many cybercriminals will be able to take advantage of this to develop their own malware without having as much advanced knowledge, which could lead to an increase in attacks of this kind.

Link

Responsible Cyber

María Pilar Torres Bruna

Cybersecurity Director at NTT DATA Latam & Perú
maria.pilar.torres.bruna@emeal.nttdata.com

Carla Passos Schawarzer

Ybersecurity Director at NTT DATA Brasil
carla.passosschwarzer@emeal.nttdata.com

Miguel Angel Garzón Ramírez

Cybersecurity Manager at NTT DATA Colombia
miguel.angel.garzon.ramirez@emeal.nttdata.com

Fernando Vilchis Rivero

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

Jose Uzcategui

Cybersecurity Manager at NTT DATA Chile
jose.uzcategui@emeal.nttdata.com

Powered by the cybersecurity NTT DATA team

es.nttdata.com