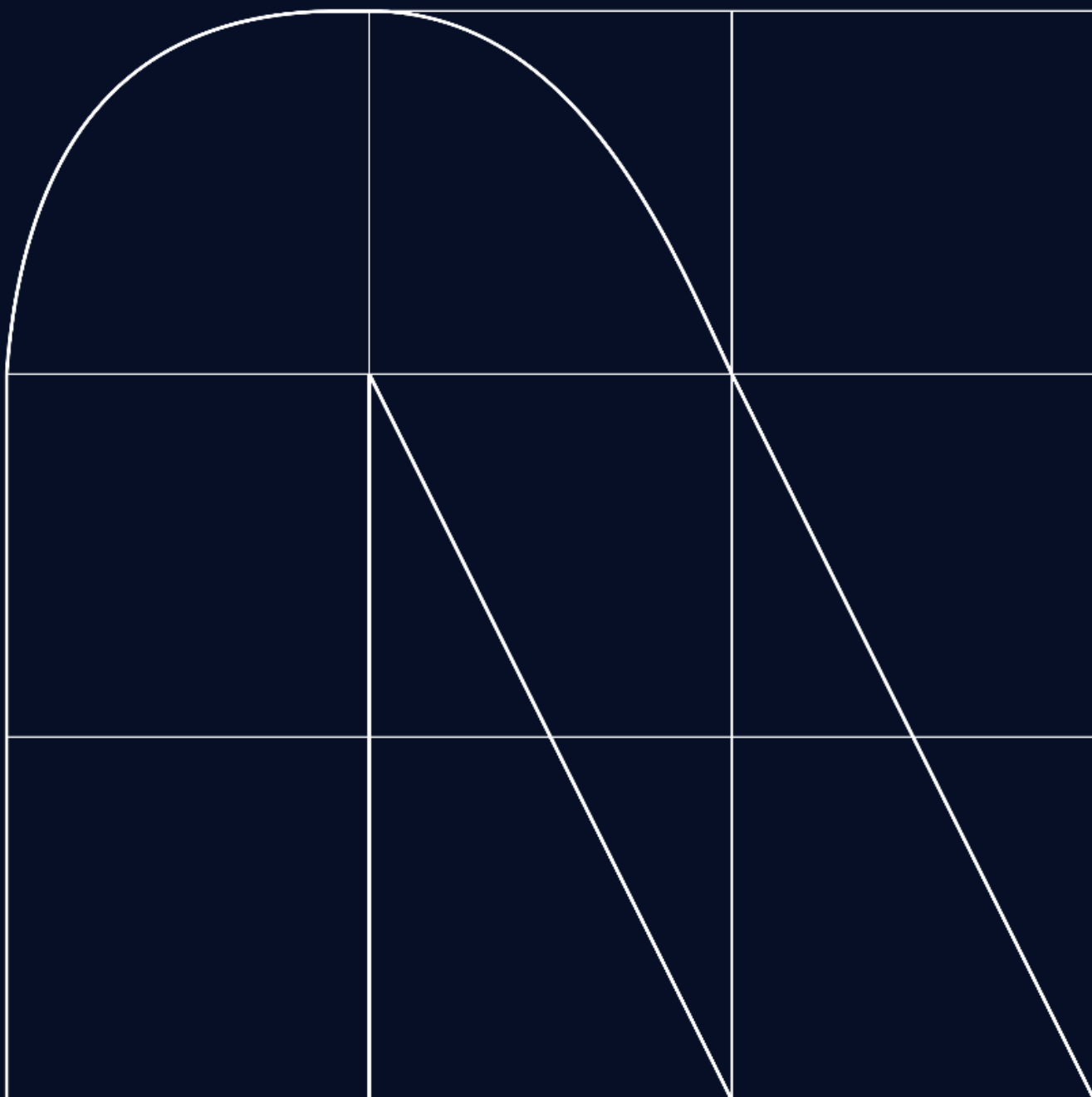
Issue 90 | May 2024

NTT DATA

Radar

Cybersecurity magazine



Integration of AI and ML in Threat Detection and Response

By Ángel Pérez y Diego Martín

In an increasingly digitised world, cybersecurity has become a primary concern for businesses, governments, and individual users alike. With the constant rise of cyber threats, the need for innovative solutions is more apparent than ever. In this context, Artificial Intelligence (AI) and Machine Learning (ML) emerge as crucial tools in the defence against these threats.

These technologies offer a proactive and adaptable approach to addressing cyber challenges. By analysing large volumes of data in real-time, AI and ML can detect patterns and anomalous behaviours, anticipating and neutralising threats before they cause harm. This predictive capability is essential in an environment where threats constantly evolve, and early detection can make the difference between a successful attack and effective defence.

From threat detection to incident response, the applications of AI and ML in cybersecurity are diverse and effective. These technologies enable security teams to respond quickly and efficiently to potential attacks, reducing human error and improving operational efficiency. Despite the benefits, implementing AI and ML in cybersecurity also faces challenges, such as the availability of adequate training data and vulnerability to adversarial attacks.

Despite the challenges, numerous companies have succeeded in applying AI and ML in cybersecurity. IBM, Darktrace, Cylance, and Fortinet are just a few examples of companies that have developed innovative solutions using these technologies to efficiently detect and prevent threats. These success stories demonstrate the potential of AI and ML to strengthen cyber defences and protect digital assets in an increasingly hostile and complex environment.

Ultimately, the integration of AI and ML in cybersecurity offers significant opportunities to enhance protection against digital threats, but their success will depend on how they are implemented and used responsibly and ethically.

For example, Symantec makes use of artificial intelligence in several of the services they offer. In their "File Reputation Analysis" service, by analysing billions of links, websites, and files, they determine whether a file is trustworthy or unsafe, thus assigning it a score before it reaches the teams.

Another example from Symantec is their "Email Security Cloud" service, which filters unwanted email messages in the cloud and protects mailboxes from targeted attacks. This service has self-learning capabilities and Symantec intelligence to provide effective and accurate email security, and is compatible with the most famous email providers.

On the other hand, they use advanced machine learning to determine the reliability of a file by recognising malicious attributes and defining rules for detections. This machine learning allows blocking new malware variants by analysing billions of examples of malicious and non-malicious files contained in the global intelligence network.

Another major company already using artificial intelligence is IBM, in their "QRADAR" suite, being a modernised threat detection and response solution. The portfolio includes enterprise-level AI and automation to dramatically increase analyst productivity, thus helping mostly teams with limited resources.
To conclude, one of IBM's other solutions implementing artificial intelligence is "IBM Security Verify". This solution implements deep AI-driven context for consumer and workforce identity access management, thus protecting users and applications inside and outside the company with a software-as-a-service approach.

Cyberchronicles

By Álvaro Ceruelo y Cayetano Valero

The European Union anticipates an increase in disinformation campaigns focused on the June European elections, originating from external actors, especially those associated with the Russian government, with the aim of interfering in electoral processes. These disinformation campaigns have adapted to the restrictions arising from the Russian invasion of Ukraine, with a predominant use of the internet and instant messaging services as means of distributing the campaigns, as opposed to more traditional channels like television, which were censored in Europe.

The identification of disinformation has become increasingly complex due to the use of the aforementioned distribution channels, as well as the very nature of disinformation, which leverages advancements in technologies like Artificial Intelligence (AI) to produce increasingly sophisticated results with less effort. Advances in this field have been reflected in recent studies, which have documented the use of generative AI for the production of text, videos, and images related to disinformation campaigns in at least 16 countries during the year 2023.

Phishing in Tax Declaration Campaign

In parallel, with the tax declaration campaign in full swing, cybercriminals are seizing the opportunity to deceive people through mass emails and messages with scams in which they try to lure someone into a trap. They are launching phishing campaigns, in which they send messages en masse, hoping someone will fall for it.

In these emails, cybercriminals use deceptive tactics, often claiming that the Tax Agency will refund you money. Additionally, they may include links to fraudulent websites that appear official but are designed to steal personal information such as card numbers and security codes. These websites are counterfeit and use logos and fonts from the Tax Agency to appear official.

It is advisable to search for the Tax Agency's website or the desired website, access the official page, and authenticate from there to check for possible notifications. In summary, online security remains a constant concern. With tax season underway, it is important to exercise caution and be vigilant about the emails and messages we receive, as many of them may be fraudulent.

Prominent Vulnerabilities

Recently, a security issue has been discovered in the XZ Utils tool (CVE-2024-3094), commonly used in Linux operating systems. This tool is used to compress and decompress data in XZ format. Andrés Freund, a developer at Microsoft, detected malicious code hidden in this tool while investigating performance issues in SSH. The malicious code modifies functions within the liblzma package and interferes with the data used by the tool, and under certain conditions, could allow an attacker to gain access to an affected system. However, this malicious code is not found in the Git distribution of the tool, only in the complete download package.

Additionally, Fortinet has released details about a critical SQL Injection vulnerability, present in versions 7.2.0 to 7.2.2 and 7.0.1 to 7.0.10 of FortiClient Enterprise Management Server. This vulnerability allows an attacker to execute commands or code remotely through specifically crafted requests, potentially gaining administrator access to the server where the software is running.

Compliance Strategies

By Soledad Romero

In an increasingly globalized world, organizations approach regulatory compliance in a variety of ways. Doing so effectively and cost-effectively requires defining a solid strategy that involves the different actors and stakeholders who need to participate in it. The complexity of regulatory compliance in a globalized world.

All organizations currently face a complex and ever-changing regulatory landscape on a global scale. The proliferation of laws and regulations across different sectors and jurisdictions presents significant challenges for entities seeking to operate within the bounds of legality. Recognizing that compliance with laws is essential to maintaining integrity and trust in institutions and markets (whether local, regional, national, or international), each organization seeks to adhere to regulations that are applicable and relevant not only to save costs, avoid cybersecurity incidents or penalties, but also with the aim of anticipating trends, strengthening its reputation, and relationships with stakeholders.

In such a dynamic environment as the present one, preparing to respond effectively is quite a challenge. Therefore, it is crucial to plan and establish a solid and well-structured compliance strategy. This not only involves identifying the level of compliance maturity within the organization but also assessing whether there is a deep knowledge and understanding of the regulation. Additionally, it is important to achieve flexibility and the ability to anticipate and adapt quickly to any new legal requirements that may arise.

In summary, regulatory compliance is a critical aspect that requires constant attention and a proactive strategy to ensure the long-term success and sustainability of any organization. This proactive strategy demands from the outset a conscious and diligent attitude among the key actors who typically intervene from its planning and functions, namely:

- Compliance Officer: Responsible for planning and executing the compliance plan and communicating the measures to be followed to the entire organization.
- Top Management: Must be committed to the compliance culture and ensure that necessary resources are allocated.
- Legal Department: Advises on legal implications and assists in interpreting applicable regulations.
- IT Department: Implements and maintains technological solutions to support compliance.
- Human Resources: Is responsible for training and raising awareness among staff on compliance matters.
- Internal and External Auditors: Verify compliance and the effectiveness of policies and procedures.
- Employees: All members of the organization must be informed and follow compliance policies.

Among the most common recommendations and best practices when establishing the strategy, we can consider the following:

1. Establish a baseline: starting with an audit to understand the current state of compliance and applicable regulations.
2. Development of procedures: that are accessible and easily applicable within the organization and reviewed periodically.
3. Monitoring and tracking: in order to ensure continuous compliance and update as needed by the entity.
4. Involvement of top management: as mentioned above regarding key stakeholders.
5. Continuous training: Employees should be well informed about regulations and how they affect their roles. In this regard, a tailored training plan should be regular and adaptable to changes in legislation.

Finally, measuring the success of a compliance strategy involves evaluating how the organization's activities align with applicable regulations and laws. Measurement through specific KPIs, surveys, risk analysis, or risk assessments, among others, provides a quantitative and qualitative insight into the performance of the compliance strategy and helps organizations adjust their practices to continuously improve.

The ultimate goal is to create a framework that addresses compliance risks and helps prevent them, ensuring that the organization is prepared for future challenges in the regulatory landscape.

We need to standardise Artificial Intelligence

By Carlos Chavarria

The use of Artificial Intelligence in the EU will be regulated by the Artificial Intelligence Act, the world's first comprehensive law on Artificial Intelligence, hereinafter referred to as AI. The Parliament's priority is to ensure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory, and environmentally friendly. AI systems must be supervised by humans, rather than by automation, to prevent harmful outcomes. The Parliament also aims to establish a uniform and technologically neutral definition of AI that can be applied to future AI systems.

Parliament and its member countries have begun drafting regulations and laws to delineate AI. Specifically, the European Parliament has pending approval for the "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS".

Among the member states, Spain is emerging as one of the main leaders following the approval on August 22, 2023, of RD 729/2023, which approves the Statute of the Spanish Agency for the Supervision of Artificial Intelligence. In addition, the AEPD (Spanish Data Protection Agency) has developed two guides on AI. The first one in February 2020 to adapt AI treatments to the GDPR and a second one in January 2021 on the Requirements for Audits of Treatments that include AI.

In this political context, the European Commission has proposed a regulatory framework on artificial intelligence with the following specific objectives:

- Ensuring that AI systems introduced and used in the EU market are safe and comply with current legislation on fundamental rights and Union values;
- Ensuring legal certainty to facilitate investment and innovation in AI;
- Improving governance and the effective implementation of current legislation on fundamental rights and the security requirements applicable to AI systems;
- Facilitating the development of a single market to enable legal, safe, and reliable use of AI applications and to avoid market fragmentation.

What problems do the application of these regulations solve?

In this context, AI presents a series of problems and risks that need to be mitigated as much as possible through EU legislation.

Due to the growing use of AI both in business and everyday life, its regulation is necessary for the following reasons:

- Ethics and individual rights: AI can have a significant impact on people's lives, from automated decision-making to the collection and use of personal data. Regulation helps ensure that individual rights are respected, and discriminatory or unfair practices are avoided.
- Privacy and security: Lack of regulation can lead to security vulnerabilities and exploitation of AI systems. Standards can be established for security and privacy to protect individuals and organizations.
- Transparency and accountability: Regulations may require transparency in AI algorithms and decision-making processes. Additionally, they can establish legal liability in case of errors or damages caused by AI systems.
- Algorithmic bias: Regulation can address bias in AI systems and ensure that unfair or discriminatory decisions are not made based on race, gender, or other factors.
- Fair competition: It can prevent anti-competitive practices and promote fair innovation in the AI market.
- Public safety: Regulations can address safety in critical applications such as autonomous vehicles and healthcare systems to avoid risks to life and health.
- Risk mitigation: AI poses significant risks, such as technological unemployment, lack of privacy, and algorithmic bias. Regulation can help address these issues and mitigate risks associated with AI.
- Public trust: It fosters public trust in AI technology, which can be crucial for its widespread adoption.
- Global coherence: Regulation can help establish common standards in an increasingly interconnected world, facilitating international cooperation and trade in AI technology.

In summary, the regulation of artificial intelligence is essential to ensure that this technology is developed and used in an ethical, safe, and responsible manner, benefiting society as a whole and minimizing risks.

When will the regulations come into effect?

The main problem when legislating in this area is that technological innovation is much faster than the time it takes to create, develop, and approve laws. Despite the growing use of AI, there is still no defined date for the approval of the EU Artificial Intelligence Act. On June 14, 2023, a series of amendments were approved in the European Parliament. Discussions have begun on the final form of the law in the Council, alongside EU countries. The aim is to reach an agreement by the end of this year.

What audit requirements will we need to meet?

Regarding the EU AI Act, since it has not yet been approved and is subject to modifications, it is too early to determine which requirements will be mandatory. As for Spain, the AEPD has published two guides on AI, among which we highlight 'Requirements for Audits of Treatments that include AI'. In it, an approach is made to a set of controls that could be incorporated into audits of personal data treatments that use AI components.

It is important to note that all included controls are designed to analyze the adequacy of the treatment from a data protection perspective. In addition, some methodological notes are added that may be specific and characteristic of these types of audits.

At a very high level, the following should be considered:

- Identification and transparency of the component
- Purpose of the AI component
- Foundations of the AI component
- Data management
- Verification and validation

What organizations will be affected by AI regulations?

All organizations that develop, market, or use AI services will be affected, but these regulations will also apply to structures that use third-party AI services or have contracts with a provider that uses AI services for the services they provide.

Additionally, when organizations consider choosing an external AI service provider in the future, they should consider some factors such as:

- Experience and expertise:
- Transparency and ethics
- Regulatory compliance
- Scalability and flexibility
- Security and privacy
- Ease of integration

In summary, we need to prepare to comply with AI regulations and ensure that our organizations are aligned with relevant regulations and standards. This will be achieved through a continuous process that requires ongoing commitment to ethics, security in development, and implementation of AI technologies.

Staying updated on changes in current and future regulations can significantly help any organization maintain compliance and avoid future penalties.

Digital Operational Resilience Act: Strengthening Cybersecurity in the European Union

By David Miguel Campos

The Digital Operational Resilience Act (DORA) represents a significant regulatory milestone for the financial sector of the European Union, aiming to strengthen the digital operational resilience of financial entities. Introduced in January 2023 and scheduled to be applied in January 2025, DORA seeks to harmonize existing regulations, focusing on the management of risks related to information and communication technologies (ICT) and resilience to severe operational disruptions. This regulation is particularly relevant in the banking and insurance contexts, where the reliance on third-party ICT services is considerable, and the associated risks can have significant cross-border implications.

The DORA framework is built upon five main pillars: ICT risk management, incident response and reporting, digital operational resilience testing, third-party risk management, and information and intelligence sharing. These pillars are designed to ensure that financial entities can effectively identify, protect, detect, respond to, and recover from cyber threats. Additionally, DORA establishes strict requirements for contracts with ICT service providers, including clauses on audit rights, subcontracting, and termination.

What are the main challenges of DORA?

The implementation of DORA presents several challenges for financial entities in the European Union. Firstly, the need for comprehensive alignment with ICT risk management requirements may require a significant review of current practices. Entities will need to establish a robust and adaptable risk management framework that addresses all aspects of digital operational resilience, from incident prevention to recovery.

Another challenge is third-party risk management, especially in an environment where many operations rely on ICT services provided by external entities. Financial entities will need to ensure that contracts with providers include rigorous provisions on cybersecurity and incident response mechanisms, which can be complex to negotiate and implement.

Additionally, DORA requires financial entities to conduct digital operational resilience testing, involving the development and execution of a series of advanced tests to assess the ability to withstand and recover from severe operational disruptions. This requires investments in technology and expertise, as well as the establishment of internal processes to conduct these tests regularly.

The notification of ICT-related incidents is also a critical aspect of this law. Entities must be able to detect and report significant incidents to relevant authorities within a short period, requiring efficient and reliable detection and communication systems.

The exchange of information and intelligence on cyber threats is another requirement of DORA that can be challenging, as it requires the implementation of secure and effective channels for information exchange between financial entities and authorities, as well as between financial entities and their peers or relevant stakeholders, while respecting confidentiality and data protection.

Finally, this regulation establishes a supervisory framework for critical ICT providers, meaning that financial entities will need to adapt to a new level of scrutiny and compliance by regulatory authorities. This may involve significant adjustments to ICT operations and governance to meet established standards.

How to overcome the challenges posed by DORA?

To overcome the challenges posed by the implementation of the Digital Operational Resilience Act (DORA), financial entities can adopt a variety of effective strategies. Firstly, it is crucial to develop a deep understanding of DORA requirements, which can be achieved through internal training and awareness programs. This includes familiarising oneself with the five pillars of DORA: ICT risk management, incident response and reporting, digital operational resilience testing, third-party risk management, and information and intelligence sharing.

A proactive approach to ICT risk management is essential, which means identifying, assessing, and mitigating risks. Entities must establish a robust risk management framework that is integrated throughout the organization, ensuring that cybersecurity measures are aligned with the entity's business objectives and risk tolerance.

Collaboration with ICT service providers is another critical aspect. Financial entities must ensure that contracts with third parties include detailed clauses on cybersecurity, audit rights, and incident response mechanisms. Additionally, conducting rigorous due diligence and continuous monitoring of providers is important to ensure compliance with DORA.

Digital operational resilience testing is critical for assessing the ability to withstand and recover from operational disruptions. Entities should implement a comprehensive testing program that includes both basic and advanced tests to identify vulnerabilities and improve response strategies.

Prompt notification of ICT-related incidents to competent authorities is a requirement of DORA. To achieve this, financial institutions need efficient incident detection and reporting systems to be able to respond quickly and appropriately.

Information sharing on cyber threats is vital for digital operational resilience. Entities should establish secure and effective channels for exchanging information and intelligence on cyber threats, both internally and with other regulatory entities and authorities.

Finally, financial entities must be prepared for the new supervisory framework for critical ICT providers established by DORA. This may require adjustments to ICT operations and governance to comply with supervisory standards.

Conclusion

In summary, complying with DORA is a complex process that requires a strategic approach and ongoing commitment to improving digital operational resilience. Overcoming its challenges requires a holistic and strategic approach, involving investment in technology, processes, and human capital. Compliance with DORA is not only a regulatory issue but also an opportunity for financial entities to strengthen their digital operational resilience and protect their operations and customers from disruptions and cyber threats. Collaboration and ongoing commitment to improving operational resilience will be crucial for success on this path.

For entities that already have ISO 27001 certification, an international standard for information security management systems, or have implemented frameworks like NIST, the path to DORA compliance may be smoother. ISO 27001 provides a framework that aligns with the risk management principles of DORA, while NIST offers guidance for identifying, protecting, detecting, responding to, and recovering from cyber threats. However, ISO 27001 certification or implementation of NIST does not equate to automatic compliance with DORA. It is essential for entities to conduct a gap analysis to identify areas where existing practices may need adjustments to meet the specific requirements of this law.

Vulnerabilities

Critical vulnerability in the XZ Utils Library

Date: April 1, 2024
CVE: CVE-2024-3094

CVSS: 10

CRITICAL

Description
Malicious code was discovered in the tarballs of XZ Utils, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a precompiled object file from a disguised test file in the source code, which is then used to modify specific functions in the liblzma code.

This results in a modified liblzma library that any software linked to this library can use, intercepting and modifying data interaction with this library.

Affected products
It has been indicated that the affected packages are only present in Fedora 41 and Fedora Rawhide within the Red Hat community ecosystem. No versions of Red Hat Enterprise Linux (RHEL) are affected.

Solution
Affected users are advised to update to versions that do not include the malicious code.

The compromised versions of the XZ Utils libraries are 5.6.0 and 5.6.1, only included in the tarball download package.

Users are advised to verify and clean their systems of these affected versions.

References
- nvd.nist.gov
- www.tarlogic.com

Vulnerability in NAS D-Link devices

Date: April 3, 2024
CVE: CVE-2024-3272 and 1 more

CVSS: 9.8

CRITICAL

Description
The vulnerabilities identified as CVE-2024-3272 and CVE-2024-3273 are rated as critical and high severities, respectively.

The critical vulnerability exists in the URI nas_sharing.cgi of D-Link NAS devices.

Currently, there is an exploit for the critical vulnerability, which could allow credential harvesting through argument manipulation. Moreover, the attack can be initiated remotely.

Affected products
The affected models by this vulnerability are those that have reached their end of life (EOL) and, therefore, no longer receive firmware updates. These include::
- DNS-340L
- DNS-320L
- DNS-327L
- DNS-325

D-Link has confirmed that these models are exposed to exploitation due to the vulnerability and recommends their removal.

Solution
Given that D-Link does not plan to release a firmware update for these EOL models, the official recommendation is to remove and replace these vulnerable devices. Users are advised that if they continue to use these devices against D-Link's recommendation, they should ensure they have the latest firmware available on D-Link's legacy website, regularly update the unique device password for accessing its web configuration, and keep Wi-Fi encryption enabled with a unique password.

References
- nvd.nist.gov
- nvd.nist.gov
- thehackernews.com

Patches

CRITICAL **Critical security updates for Google Chrome**

Date: April 2, 2024
CVE: CVE-2024-3156 and 2 more

Description

Google has released a series of security updates to address several issues affecting the Google Chrome product. The update fixes a total of 3 vulnerabilities, all of which are critical in severity.

The CVE-2024-3156 vulnerability, categorized as an inappropriate implementation in Google Chrome's V8 JavaScript engine, could be exploited to execute arbitrary code or access sensitive information on the system.

The CVE-2024-3158 vulnerability occurs when a program accesses a memory area after it has been freed, which could result in unpredictable behavior or unauthorized code execution.

The CVE-2024-3159 vulnerability also affects the V8 JavaScript engine due to incorrect memory access out-of-bounds, which can lead to unpredictable behaviors through specific JavaScript manipulations or even allow the execution of malicious code.

Affected Products

The versions of Google Chrome affected by these vulnerabilities are:

- Versions prior to 123.0.63.12.105, 123.0.63.12.106, and 123.0.63.12.107 for Windows and Mac.
- Versions prior to 123.0.63.12.105 for Linux.

Solution

Update Google Chrome to the latest available version for Windows, Mac, and Linux from the official website.

References

- chromereleases.googleblog.com
- www.bleepingcomputer.com

CRITICAL **Android Pixel/Nexus April Security Update**

Date: April 2, 2024
CVE: CVE-2024-29740 and 2 more

Description

The Android Security Bulletin of April 2, 2024, highlights several security vulnerabilities detected on Pixel/Nexus Android devices of critical and high severity.

Among all the detected vulnerabilities, it is worth noting 1 critical severity and 2 high severity (zero-day) vulnerabilities, detailed below:

- CVE-2024-29740 (critical): Privilege escalation vulnerability on the mentioned Pixel devices.
- CVE-2024-29745 (high): Vulnerability that may lead to disclosure of confidential information.
- CVE-2024-29748 (high): Privilege escalation vulnerability.

Affected Products

You can consult the complete list of affected products, which impact compatible Pixel devices, at the following link: support.google.com.

Solution

The solution to these vulnerabilities involves applying platform-level security patches provided by the Android Open Source Project (AOSP).

Pixel phones receive updates to address security issues detailed in Android's public security bulletins. It is recommended to check and update to the latest version of Android Pixel as indicated on the official page.

References

- cybersecuritynews.com
- bleepingcomputer.com

Events

RSA CONFERENCE 2024 SAN FRANCISCO (6 May – 9 May)

The RSA Conference, founded in 1991 by RSA Security, has emerged as one of the most important conferences in the field of cybersecurity globally. This flagship event brings together experts, industry leaders, and IT professionals to address current and emerging challenges in computer security. Through presentations, panels, workshops, and demonstrations, the conference provides a vital space to explore new solutions and best practices in data protection, cyber threats, cloud security, artificial intelligence applied to security, regulatory compliance, and other key topics in information protection. The RSA Conference has become an essential platform for collaboration, learning, and innovation in an increasingly interconnected digital world.

Enlace

XIII CYBERSECURITY FORUM (14 May)

The XIII Cybersecurity Forum, organized by ISMS Forum Spain and its working group Cyber Security Centre (CSC), will take place in Madrid on May 14th, 2024. The event will address the latest trends and challenges in cybersecurity, with a special focus on data protection, risk management, and incident response. The program includes presentations by experts, roundtable discussions, and practical cases, making it a must-attend event for those seeking to learn about the latest trends and solutions in cybersecurity.

Enlace

OSINTOMÁTICO CONFERENCE 2024 (17 May – 18 May)

The Osintomático 2024 conference brings together security professionals, researchers, and enthusiasts to share knowledge about open-source intelligence (OSINT) techniques and social engineering. The program includes presentations, workshops, roundtable discussions, and hands-on demonstrations on topics such as gathering information from open sources, analyzing social media data, background investigation, and cybersecurity. The speakers are recognized experts in their fields, and the conference is an excellent opportunity to learn and network with other industry professionals.

Link

BARCELONA CYBERSECURITY CONGRESS (May 21 – May 23)

The Barcelona Cybersecurity Congress, in its 2024 edition, establishes itself as a key event in the field of digital security in Spain. Under the motto "Cybersecurity in the Digital Era: Comprehensive Protection and Resilience," this congress will provide both an in-person and virtual platform to address current and future challenges in the field of cybersecurity. With a comprehensive approach, crucial topics such as digital identity, data protection, and risk management in an increasingly interconnected environment will be explored.

Link

45TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY (22 May – 24 May)

Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for presenting advances in computer security and electronic privacy, and for bringing together researchers and professionals in the field. The 2024 Symposium will mark the 45th annual meeting of this flagship conference. The Symposium will take place from May 20th to May 22nd, 2024, and the Security and Privacy Workshops will be held on May 23rd, 2024. Both events will be held in San Francisco, California, at the Hilton San Francisco Union Square.

Link

IX NATIONAL CYBERSECURITY RESEARCH CONFERENCE (27 May – 29 May)

JNIC is a scientific congress that promotes the exchange and discussion of ideas, knowledge, and experiences between the academic and research network on one hand, and professionals and companies on the other. It serves as a showcase for the latest scientific advances in the field and materializes a forum for debate where innovative perspectives and approaches in cybersecurity can be presented, enabling the connection between research and innovation and the development of products and services of value to society. Researchers and professionals from different parts of the country will present the results of their scientific research from various perspectives with a common thread: cybersecurity. The Conference will focus on three pillars: Research, Transfer, and Training in Cybersecurity.

Link

Resources

EVOLVING DATA THREATS IN 2024

In this digital era, data has become one of the most valuable resources for businesses, governments, and individuals alike. However, as our dependence on data increases, so do the threats and risks associated with it. In the year 2024, a series of new challenges will emerge at the forefront of data security, and cyberattacks will become more advanced, complex, and severe.

Link

IS THE CYBERSECURITY INDUSTRY READY FOR AI?

In recent years, there has been a significant increase in interest surrounding the crucial role of artificial intelligence in cybersecurity, as well as the notable benefits it provides to cybersecurity business strategy. However, this article addresses the fundamental question of whether the cybersecurity sector is adequately prepared to deal with all the complexities inherent in AI, beyond its obvious benefits.

Link

CYBERSECURITY MEASURES TOOLKIT

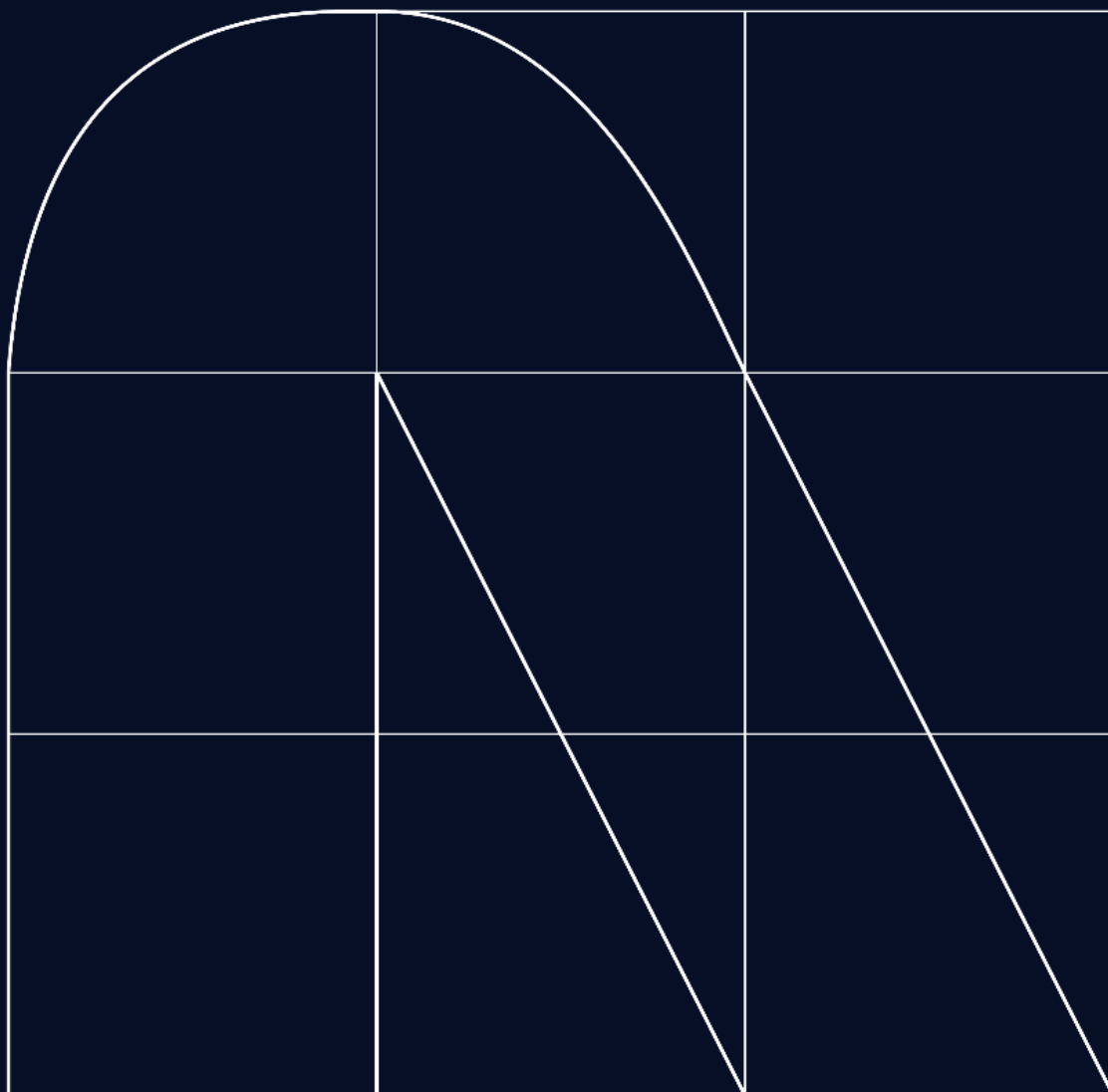
In order to strengthen EU solidarity and its capabilities to detect cybersecurity threats and incidents, prepare for them, and respond when they occur, as well as to enhance its cyber resilience, the Presidency of the Council and negotiators from the European Parliament have reached a provisional agreement on the so-called Cyber Solidarity Regulation and a specific amendment to the Cybersecurity Regulation.

Link

THUNDERSTRIKE: RUNNING MALICIOUS APPLICATIONS UNNOTICED IN THE FACE OF MODERN ANTI-MALWARE SOLUTIONS

NTT DATA's commitment to innovation intensifies with every step we take. At the recent RootedCON Congress, one of the most prominent events in the Spanish-speaking sphere, our colleagues Antonio Pérez Sánchez and Marcos González Hermida presented Thunderstrike, an innovative tool.

Thunderstrike is a post-exploitation tool with advanced evasion techniques that enables the loading and execution of .NET applications, such as Seatbelt and Rubeus, among others. This tool is capable of doing so without being detected by modern anti-malware systems: Endpoint Detection and Response (EDR) systems.



Powered by the cybersecurity NTT DATA team

es.nttdata.com