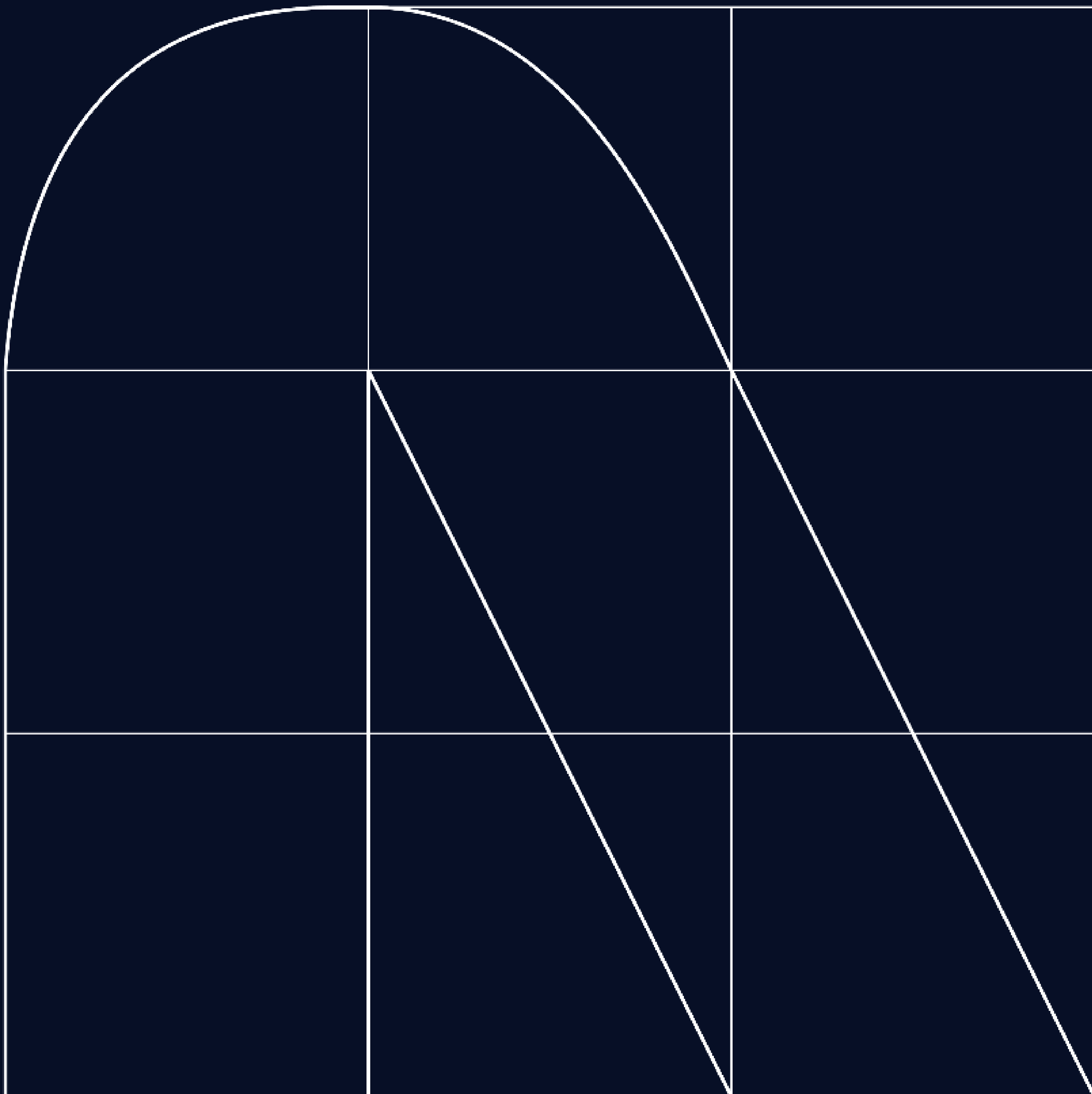
Issue 89 | April 2024

Radar

Cybersecurity Magazine



Security in applications and artificial intelligence

By Roberto Junior Ruiz Neyra

More than 50% of malware reaches users through cloud applications. Many of them have geopolitical origins, while others originated from cybercriminals such as the Russian group Wizard Spider, TA505, FIN7. Among the main victims of these attacks are financial services and healthcare. Most of these situations occur due to security breaches in the applications where cyber attackers exploit vulnerabilities to inject malware and achieve their goal.

The genesis of this phenomenon lies in the security integrated into the design of these applications, extending through to their own development. The latest studies have shown that over 70% of developed applications contain security breaches, representing a significant risk to organisations. This risk is exponential when applications have a wide commercial reach, turning several companies and countries into potential victims. An important point to note is that, as generative AI gains prominence in software development, the risk of vulnerabilities increases if this practice is not controlled. This is due to the code being written by large language models trained on uncleaned data sources, such as public GitHub repositories. Therefore, it is super important to verify the security of the new application through Static Application Security Testing (SAST) tools and Software Composition Analysis (SCA) tools managed by Cybersecurity specialists in order to maximise the identification of flaws or vulnerabilities and correct them, allowing developers to make the most of the benefits of AI without compromising the security of the applications.

Fortunately, the era of AI not only comes to gain ground in the software development field but also in the field of application security. For instance, within the DevSecOps and Cloud Security practices, new solutions are emerging that cover use cases such as vulnerability interpretation and proposing remediation scripts for these vulnerabilities in real time. Another interesting use case is training AI to conduct security testing through attack simulation. Like these examples, there are others where we can have AI as an ally to ensure the development and creation of applications.
At NTT DATA, we are convinced that AI will be key to evolving and innovating security in applications where we contribute to agility in "time to market", do not affect the user experience when strengthening security, and remain firm with the principle of Zero Trust

Roberto Junior Ruiz Neyra
Cybersecurity Manager

Cyberchronicle

By Christian Agreda

We begin this month's cyberchronicles by discussing the SmartScreen zero-day vulnerability in Windows Defender (CVE-2024-21412) that was discovered.

This vulnerability arises from a failure in applying the "Mark of the Web" (MotW), a security feature used by Windows to identify files originating from potentially untrusted sources such as internet downloads, WebDAV, and SMB shares. Under normal circumstances, files downloaded from the web are tagged with MotW, causing Windows Defender SmartScreen to issue alerts when such files attempt to run or when a user tries to execute them directly. This mechanism acts as a critical defense, preventing malicious or unauthorised code from running without the user's knowledge or consent.

However, CVE-2024-21412 allowed attackers to bypass these protections by exploiting a flaw in the handling of Internet shortcuts (.URL files) and other mechanisms. Through phishing campaigns and the use of compromised websites, attackers distributed these malicious .URL files. When executed, these files lacked the MotW label, effectively blinding SmartScreen to their malicious intentions. This oversight allowed the DarkMe malware to run without triggering the usual security warnings that would alert users to potential danger.

By bypassing SmartScreen's defenses, Water Hydra was able to execute its attack chain discreetly, infecting victims' machines without detection. The attack exploited the trust that Windows places in files lacking the MotW designation, assuming they are safe and originate from a trusted source within the user's environment. This exploitation represents a significant breach of trust in the security mechanisms designed to protect users from the same type of orchestrated attack by Water Hydra.

Connectwise recently addressed two critical vulnerabilities (CVE-2024-1709 and CVE-2024-1708) in all on-premises versions of ScreenConnect prior to 23.9.7 with an urgent security patch released on February 19, 2024 [9]. CVE-2024-1709, an authentication bypass vulnerability rated 10/10 in severity, compromises ScreenConnect by allowing unauthorised users to manipulate the URL access (e.g., /SetupWizard.aspx/anygivenstring) to the setup wizard, potentially gaining full administrative privileges and executing arbitrary code.

A critical vulnerability, identified as CVE-2023-22527, was discovered in Atlassian Confluence, posing a serious security risk with a CVSS score of 10 [10]. This vulnerability stems from a template injection flaw within the Object-Graph Navigation Language (OGNL), a widely used component in web applications for creating server-side templates. The exploitation method involves attackers targeting specific .vm template files within Confluence, which mishandle user-provided input. For example, the vulnerability was identified in the /confluence/template/aui/text-inline.vm file, where attackers could inject malicious code through parameters intended for legitimate page functions. This file, among others, failed to properly sanitise input, allowing attackers to remotely execute commands on the affected system.

To address this vulnerability, Atlassian has released updates for Confluence Data Center and Server, particularly version 8.5.4 and later, which include patches to mitigate the risk of exploitation. These updates correct the vulnerability by ensuring that user input is properly sanitised and by removing or protecting the affected template files.

We conclude our cyberchronicles of the month by addressing an Exchange vulnerability. Exchange administrators may have enjoyed a rare two-month respite from patching, but this month sees the disclosure of CVE-2024-21410, a critical privilege escalation vulnerability in Exchange. Microsoft explains that an attacker could use previously acquired NTLM credentials via other means to act as a victim on the Exchange server through an NTLM relay attack. One possible avenue for such credential acquisition: an NTLM credential leakage vulnerability in Outlook like CVE-2023-36761, which Rapid7 wrote about in September 2023.

To compound defenders' concerns: Exchange 2016 is listed as affected, yet no patch appears in the CVE-2024-21410 advisory. Exchange 2019 patches are available for CU13 and the new CU14 series. According to Microsoft, the Exchange installations where Extended Protection for Authentication (EPA) is already enabled, are protected, although Microsoft strongly recommends installing the latest cumulative update. Additional resources are provided in the advisory, including Microsoft's generic guidance on mitigating Pass the Hash-style attacks, as well as Microsoft's Exchange Server Health Checker script, which provides an overview of EPA status. The Exchange 2019 CU14 update series enables EPA by default.

A day after the initial disclosure, Microsoft updated the CVE-2024-21410 advisory to indicate that they were already aware of exploitation.

Christian Agreda Romero
Cybersecurity Lead Analyst

Information Security Integration into Organisation's Daily Operations - The Case of DevSecOps

By Notis Iliopoulos

The transition to the new digital reality, led by major digital transformation programs, alongside rapid change, and adoption of the supporting technology, highlights the need to implement one of the fundamental principles of information security: integrating information security responsibilities into every job role. This article focuses on incorporating information security requirements into software/system development and information system operations, exploring how this can be achieved through the adoption and practical implementation of the DevSecOps approach.

DevOps has already been embraced as a standard process aiming to bridge the collaboration gap between software development departments and IT infrastructure operations departments, to enhance software reliability, streamline the deployment cycle of new versions (CI/CD), and reduce deployment time. The DevOps process, serving as a precursor to DevSecOps, was swiftly adopted by software development companies and organisations heavily reliant on IT systems and applications. However, it was quickly realised that information security requirements, regulatory compliance, personal data protection, and software resilience (collectively referred to as information security) must be part of the DevOps process. Consequently, the DevSecOps philosophy emerged, encompassing all these critical aspects.

The speed and frequency at which new software versions are developed and made available demonstrate that traditional methods of managing information security, privacy protection, and regulatory compliance are ineffective and obsolete. The adoption of the DevSecOps approach aims to introduce a new process that integrates information security requirements throughout the software development lifecycle, also considering more flexible Agile software development methodologies. This process represents a natural evolution of the DevOps process and aims to incorporate information security requirements at every step of the new agile software development methodologies. Therefore, information security requirements are part of every software development cycle (sprint) and are not only addressed at the end of the software development process, as in traditional methods.
A fundamental principle of the DevSecOps process is to foster a culture, followed by a relevant implementation methodology, where information security requirements seamlessly integrate into software development, installation, and support processes.

Therefore, current, and old practices require adjustments or replacement with an approach that easily adapts to ensure the inclusion of all information security requirements in a repeatable process that easily adjusts to the current dynamic technological landscape. Considering this, information security should be viewed as a service provided at each phase of the lifecycle of developing new software products or during the CI/CD process of existing software applications.

Therefore, constant adaptation of the process, its smooth and repeatable operation, and its automation become an essential requirement. Key information security requirements for each phase of software development that should be included in the DevSecOps process are presented below:

Design and Analysis: During the design phase, the implementation team identifies information security needs for each project stage and assigns relevant responsibilities to engineers with appropriate skills. At the same time, an initial assessment of related information security threats and risks (threat profiling) is conducted to define information security requirements and specifications for the final deliverable (new product or new version). An effective way to achieve this is by drafting and documenting the "Security Plan" of the product under development, which includes information security threats, potential vulnerabilities, and proposed protection measures. Additionally, the plan should address requirements for both personal data protection and regulatory compliance.

Architectural Product Design: Adoption of the "Security by Design" philosophy, whereby each product or each new version of the product is designed from the outset, taking into account best practices of information security, concerning every component of the product, from source code to the infrastructure on which it will be installed and operated. During architectural design, the aforementioned "Security Plan" serves as the primary tool to design necessary security measures and consider relevant regulatory compliance requirements.

Development and Source Code Review: The main concern is the continuous improvement of the quality, security, and resilience of the final product through source code. To achieve this, developers need continuous training in secure and resilient programming practices. In addition to training, documented source code security guidelines are required, which developers must rigorously adhere to. Throughout the source code development phase, the mentioned principles should be known and implemented by software engineers.

Software Security Review: Periodic review of the generated source code to identify potential information security vulnerabilities and resilience issues should be considered as part of the responsibilities of software development teams. This can be achieved through a combination of automated tools and manual verifications, which should be part of regular software inspection practices.
Unlike traditional methods, where software security reviews are conducted at the end of the development phase by a particular team, the DevSecOps process integrates security reviews throughout the development phase. This allows for early identification and remediation of information security vulnerabilities. Additionally, organisations adopting the DevSecOps process must further develop and improve information security controls related to software development, due to the adoption of agile software development methods allowing for the continuous integration and deployment of new software versions.

In such an environment, it is necessary to include all required controls to assess the security of the new software or release as early as possible. Assessments should identify potential security vulnerabilities both in the software's logical flow and in communication between its different components, including interactions through programming interfaces (APIs). Such assessments can be conducted using automated tools (dynamic source code analysis) and penetration testing exercises. Furthermore, these assessments should be incorporated into the default test scenarios of the final deliverable, ensuring comprehensive management of assessments and tests conducted at each stage.

Installation: The deployment of the new version of a software product in the production environment is carried out through automated processes, ensuring a secure and reliable deployment of the latest version. Additionally, it is crucial to strengthen the security level of the production environment where the product is installed, according to the importance of the hosted data and applicable best practices.

Operation: During the operational phase of the new software, automated processes are used to detect technical security vulnerabilities. This involves the use of monitoring systems to detect malicious attacks, intrusion detection systems, and security vulnerability scanning systems. This way, the effectiveness of controls against potential technical weaknesses that malicious attackers could exploit is increased. At the same time, real-time information is collected to identify potential security breaches in the production environment, including violations related to the software. Any defect or vulnerability identified through monitoring is reported to the operations engineers of the production environment for resolution, ensuring continuous improvement, increased reliability, and security of the product.

Pitfalls to Avoid

Adopting the DevSecOps philosophy is a process in itself, requiring careful planning and smooth implementation. To enhance the effectiveness of the process and facilitate its integration into the existing operational environment, we recommend avoiding some significant obstacles:

Focusing solely on automating parts of the DevSecOps process: To fully leverage the benefits of DevSecOps, information security requirements must be part of every stage of the software development lifecycle. As a first step towards adopting DevSecOps, it is recommended to form an interdepartmental team of experts who actively participate and contribute to all phases of the software development lifecycle, while optimising the process by adding necessary automation to support it. Failure to gain management support: To ensure management support, it is necessary to highlight the advantages of adopting the DevSecOps process. This includes emphasising the increased effectiveness of the overall software development and deployment process, as well as the enhanced level of security and reliability of the product or version.

Applying DevSecOps practices only to the development of new products: Adopting the DevSecOps process is facilitated during the development of new software products; however, its immediate value to the organisation can be realised by applying it to existing software products, showing immediate results such as maximising flexibility, security, and reliability of new product releases. Therefore, the added value of the new process must be understood and applied as a priority in areas that directly demonstrate its utility.

Inability or failure to create the necessary culture and relevant skills: The lack or failure to establish the right culture and develop the necessary skills: Implementing the DevSecOps process involves a cultural shift, where everyone involved in product development assumes responsibility for information security, reliability, and resilience, rather than delegating it to a specific team. Additionally, training and developing the necessary skills are crucial for the overall success of DevSecOps adoption.

Effective Adoption and Evolution of the DevSecOps Process

The most significant change impacting current working methods is establishing a horizontal interdepartmental team. This team will consist of professionals with different skills who typically work in different organisational units, vertically focused on specific areas of expertise. This implies the need to eliminate organisational silos. Furthermore, it requires dismantling organisational silos that traditionally separate different teams and departments within an organisation. It is necessary to create a permanent organisational unit or a multifunctional virtual DevSecOps team composed of professionals with specific skills from different departments.

Clearly, the most significant change an organisation must undergo is cultural. This encompasses operation, level of agility, and the services that the DevSecOps process aims to deliver. Therefore, the organisation needs to identify those who can contribute to and promote this change in terms of mindset and way of working and designate them as key members of the DevSecOps process. This will lead to the formation and operation of a multifunctional team, either as a fully autonomous entity or a virtual task force. The primary goal is to transfer all knowledge gained throughout the organisation, ensuring that information security becomes an integral part of the design and development of new software products and versions.

DevSecOps teams, whether autonomous or virtual, should be composed of engineers with diverse skills, capable not only in their domains of expertise but also of continually enriching their capabilities. This enables them to effectively execute a variety of interconnected tasks within the development of a new product or a new software version. These tasks include software development, implementation and optimisation of information security controls, and maintenance and support of IT infrastructure. Each team member is responsible for the security and reliability of the product, whether for external customers or internal use.

The DevSecOps process, from its inception phase, should serve as a robust framework, offering services and creating methodologies, procedures, and tools that can be used with or without the involvement of DevSecOps team members. At the same time, DevSecOps team members should enhance the effectiveness of the services and tools they use, as well as train and mentor other engineers on information security, resilience, and reliability of software.

Conclusion

DevSecOps is governed by a new philosophy that leads to a new approach in developing new products and new software versions. In most cases, there is no need to create a specific organisational unit dedicated to DevSecOps activities. The effectiveness of the new philosophy/process is maximised once it becomes a conventional way of working and is integrated as a standard part of the culture regarding the development of new products and software releases.

According to recent predictions and trends, there is broader adoption of the philosophy that will transform DevSecOps into BizDevSecOps. This is a new approach to software product development that eliminates boundaries between the business world and technical teams, with the aim of empowering businesses to build faster and more reliable software products tailored to end-user needs.

Notis Iliopoulos
Senior Manager
Cybersecurity EMEAL

SECURE APPLICATIONS IN AN IAM MANAGEMENT SYSTEM

By Mijail Muñoz

In the securing of applications, a key line is Identity and Access Management (IAM). One of the attackers' focuses is stealing the user's identity to execute fraudulent operations. Against this, raising awareness among all employees must be one of the main cybersecurity strategies in an organisation.

Currently, there are various user attack factors within an organisation, some of the better-known ones being:

- Phishing: User attack through email.
- Ransomware: Malicious software that disables the device and encrypts information.
- Spyware: Program installed on the computer to collect user information.
- Trojan: Malware that can be the transmission vehicle for a virus used for spying, data theft, or taking control of the device.
- SQL Injection: A type of cyberattack affecting company servers, infecting them, and extracting relevant information such as customer data, bank accounts, and passwords.
- Denial of Service (DoS): Its goal is to overload a website's server to render it unusable.

Implementing secure applications in an IAM system helps strengthen security, ensure compliance with regulations, and improve efficiency in identity and access management. It is important to stay updated with security best practices and adjust policies as organisational risks and needs evolve.

To ensure security in an IAM system (Identity and Access Management), it is important to use applications that adhere to the best security practices. Specifically, it must be ensured that applications have:

1. Automated Provisioning and Deprovisioning:
Automating user account creation, modification, and deletion helps avoid human errors and ensures consistency in applying security policies.

2. Role-Based Access Control (RBAC):
Using RBAC models ensures that users only have access to the resources and data necessary to perform their specific functions. This minimises risks associated with unnecessary access.

3. User Activity Monitoring:
Recording and monitoring user activities helps detect unusual behaviour or malicious activities. This is crucial for complying with security regulations and responding quickly to threats.

4. Multiple-Factor Authentication (MFA):
Implementing MFA adds an additional layer of security by requiring more than one form of authentication. This significantly reduces the risk of unauthorised access even if user credentials are compromised.

5. Password Management:
Implementing strong password policies and using password management tools can improve security without sacrificing usability.

6. Identity Federation:
Allows users to access multiple systems and applications with a single identity, reducing the need to manage multiple credentials. This can also improve security by centralising authentication.

7. Auditing and Reporting:
Conducting regular audits and generating detailed reports on user activities and changes in privileges helps meet compliance requirements and identify potential security issues.

8. Session Management:
Monitoring and managing user sessions can prevent unauthorised access, especially in sensitive environments. Implementing automatic logout after periods of inactivity is also advisable.

9. Access Policy Automation:
Automating the application and updating of access policies helps ensure that changes are made consistently and timely, reducing the risk of misconfigurations.

10. Data Encryption:
Implementing encryption to protect confidential data, both at rest and in transit, ensures that only authorised users can access sensitive information.

11. Cloud Identity Management:
If cloud services are used, securely managing identities and access is essential, adapting to the specific cloud security models.

Cybersecurity is a constantly evolving field, so it is essential to stay abreast of the latest trends, threats, and IAM solutions. Therefore, it is advisable for companies to conduct IAM Assessments of Organisational Units or applications periodically, with the purpose of finding improvement points in the 06 domains (Account Management, Authentication Management, Policy and Procedure Management, Role and Permission Management, IAM System Management, and Privileged Account Management) and adapting their access control and identity system to both new threats and the evolution that the organisation has undergone since the last assessment.

Mijail Muñoz
Cybersecurity IAM Leader

AI: Beyond the industrialisation of security tasks in the software development lifecycle

The integration of Artificial Intelligence in the software development industry is a reality that is here to stay. Currently, there are many providers competing to be the first to introduce AI in the automatic detection and correction of vulnerabilities in their clients' software development lifecycles.

The disruption of Artificial Intelligence in the software development market is causing a shift in how organisations tend to industrialise their quality and security testing during the Software Development Lifecycle (SDLC).

There are many uses being given to AI, with more or less lawful purposes, which has sparked a debate about the need for regulation of this nascent technology. In any case, the wide variety of options provided by different AI applications translates into interesting alternatives for creating tools from a cybersecurity perspective.

Although cybersecurity currently heavily relies on human input, we are gradually seeing technology becoming better than us in specific tasks, which is why AI is starting to be integrated for various purposes:

- Automatic detection and alerting of attacks in real-time.
- Data protection in hybrid environments (Legacy and/or Cloud).
- Automatic classification of vulnerabilities and risk assignment through machine learning.
- Identification of security best practices during development.
- Provision of security recommendations for addressing vulnerabilities or defects.
- Identification of security requirements.
- And many other purposes imaginable.

Regarding the SDLC, organisations are exploring different avenues to automate tasks in the various phases:

1) Requirements.
2) Design.
3) Implementation/development.
4) Testing and verification.
5) Deployment.
6) Operation.

The alternatives provided by AI at the level of automated tools are also triggering significant advancements in SecDevOps environments, leading to the evolution of what we currently know as Application Security Testing (AST) tools. These tools are beginning to replace their search engines with AI, giving them better cognitive performance to detect defects and vulnerabilities in the different phases of the SSDLC.

Many AST tool providers are developing integration modules with ChatGPT or developing their own AI, harnessing the power that this technology offers. Thanks to AI, there is no need to develop rule engines and/or policies to detect patterns or flows in the code, as the AI database itself will respond to defects that may be found in the code, in the running application, or in the environments

Therefore, the direction that the automation industry is taking is towards the development of simple modules that query AI, leaving complex decision-making tasks and cognitive power to it. These modules will function as APIs, translating different queries into a language understood by the AI being used. This way, we will be able to cover security testing in all phases of the SDLC, using:

- Modules that query AI for establishing the security requirements of the software to be designed based on a series of parameters determined by the needs to be met (technologies to be used, languages, libraries, components, environments, platforms, integrations, etc.).
- Integrations with IDEs to detect defects in real-time during development, marking them and providing developers with alternatives to address them.

- Modules for identifying improvements to implement in the SDLC itself based on recurring errors, vulnerabilities, findings, or defects.
- Awareness and/or training initiatives for developers based on the technologies used and the defects and vulnerabilities found.
- Development of tools for querying vulnerabilities in code, libraries, or at runtime.
- Modules for automatically detecting malware signatures and automatic incident response.
- Prediction of attacks based on software or system behaviours.
- Automation of event, alert, and/or vulnerability categorisation.
- And countless other needs not yet addressed by organisations and that can be addressed by developing a simple module that performs the translation of a query to AI.

We are convinced that these integrations of AST tools with AI will bring greater efficiency to software security review tasks, ultimately resulting in significant cost savings.

Looking at its trajectory, AI will likely reduce "False Positives or False Negatives" in findings, as well as alert and event fatigue. It is also allowing for the improvement of processes for automatically categorising and classifying such findings, which again impacts the agility of secure software development tasks.
However, despite the power that modern AI is beginning to present, it is still not capable of interpreting results with the same capabilities as a human being, so we must continue to review these results for possible "False Positives or False Negatives".

In this sense, security teams should not fear being replaced by AI (at least for now), as human teams will still be necessary for operation, result review, and decision-making. However, as is customary in the field of cybersecurity, the real challenge will be to continue to retrain, investing in staying updated on new market trends and the future of technology. The sector needs more cybersecurity experts specialising in AI, capable of innovating in the integration of both worlds and obtaining the differential performance expected from this technology.

At NTT DATA, we are convinced that the integration of AI into SecDevOps environments is a reality that is still taking shape because, although work is being done today, AI has yet to govern, it is a powerful tool, but it needs to stabilise to gain trust. AI is also maturing, establishing trusted environments, closed models that do not share data, and will allow greater privacy, making AI mature and enabling its inclusion in productive and industrialised environments.

We are walking down a path that appears exciting and motivating for those of us working in technology companies. At a time when the evolution towards the Cloud is paramount, along with automation and industrialisation, revolutionised by the cognitive power of AI. Under this scenario, security teams will have to give 200% to address the new paradigm.

Jose Carlos Moral Cuevas
Chief of Security Architecture
Area & Technical Manager

Increasing Application Security Through Security Chaos Engineering

Trends

It is likely that all existing applications worldwide have experienced some sort of failure that has caused trouble for more than one person. In 2011, Netflix introduced the concept of chaos into its systems in order to assess their resilience; by randomly shutting down EC2 instances on AWS, they were able to determine that their load balancers were not functioning efficiently. Nowadays, this powerful idea has been transferred to cybersecurity, offering an innovative perspective for discovering vulnerabilities in applications.

Security Chaos Engineering involves deliberately introducing security failures into applications to analyse the behaviour of their components. This concept represents a shift in the way system security is audited, enabling the identification of risk scenarios that are not easily detectable.

Currently, software development lifecycle productivity has been leveraged on DevOps practices, where rapid building and delivery of functionalities are essential for ensuring digital transformation. Likewise, security has been enhanced by integrating static and dynamic analysis tools that allow for quick identification of vulnerabilities.

However, excessive reliance on tools can be counterproductive, especially when scanning engines are not robust enough or when development teams can manipulate configurations. This is where Ethical Hacking continues to play a fundamental role in discovering breaches that cannot be identified through automation.

If there are automated security tools and Ethical Hacking to test applications, what is the contribution of Security Chaos Engineering? The power of this concept lies in its methodology, as it is based on the discovery of vulnerabilities through the scientific method. Just as Pasteur discovered penicillin through observation of an event, formulation of a hypothesis, and execution of an experiment, it is possible to discover new risk scenarios in applications.

Imagine the following scenario: a software developer's account has been compromised by an adversary due to weak credentials and the absence of multi-factor authentication; The adversary aims to infect the application repositories with malicious code in order to gain access to the organisation's servers. Will the DevOps ecosystem (processes, tools, and people) be able to detect, prevent, and mitigate this type of attack vector?

SolarWinds assumed so; however, their static analysis tool did not detect the malicious code, their stakeholders did not alert about developers self-promoting code to main branches, nor were unjustified variations in server performance detected, let alone unconventional packet traffic on their network, triggering the Supply Chain Attack with the greatest impact in decades, affecting over 20,000 companies worldwide.

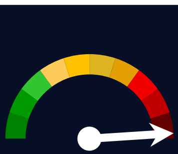
Security Chaos Engineering provides the possibility to inject security failures into source code, libraries, servers, and even into the architecture of a system in order to determine if the organisation is prepared for targeted attacks. Furthermore, Security Chaos Engineering promotes automation, so it is ideal for hypotheses, observability, and experiments to be automated through scripting in order to be tested in different applications and scenarios.

With the rise of digital transformation, cyberattacks are becoming increasingly sophisticated and require new mechanisms of protection and prevention. Security Chaos Engineering emerges as an innovative paradigm that challenges the security of systems and thereby contributes to maintaining a resilient and secure technological ecosystem.

Vulnerabilities

Code injection vulnerability in PostgreSQL

Date: March 06, 2024
CVE: CVE-2024-27304



CVSS: 9.8

CRITICAL

Description

Pgx is a Go library designed to interact with PostgreSQL databases. The identified security risk consists of the possibility of SQL code injection when an attacker manages to make a query or binding message exceed 4 GB in size.

This issue is due to an integer overflow in the size calculation, allowing a large message to be split into multiple messages under the control of the adversary.

The manufacturer has urged users to update to the latest version to fix this vulnerability. Additionally, rejecting requests that exceed a certain size is proposed as a temporary measure.

Affected products

The vulnerability affects the PGX product, specifically the following versions:

- Versions prior to 4.18.2.
- Versions between 5.0.0 and 5.5.3, these two inclusive.

Solution

Users are advised to update to versions 4.18.2 or 5.5.4 to protect themselves against potential attacks.

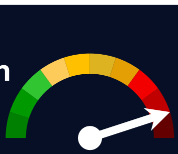
Additionally, it is also recommended to reject any user input that may result in a single query or binding message exceeding 4 GB in size, mitigating the risk of exploitation of this vulnerability.

References

- www.incibe.es
- nvd.nist.gov

Privilege escalation vulnerability in Microsoft AKS

Date: March 12, 2024
CVE: CVE-2024-21400



CVSS: 9

CRITICAL

Description

Microsoft Azure Kubernetes Service (AKS) is a Microsoft Azure management service that allows users to easily deploy, manage, and scale Kubernetes-based container clusters in the Azure cloud.

Vulnerability CVE-2024-21400 consists of a privilege escalation in the official container of the Microsoft Azure Kubernetes service. The discovered vulnerability allows attackers to gain unauthorized access to resources that are protected within a Kubernetes cluster. This could lead to manipulation of sensitive data, service disruption, or even total compromise of the cluster.

Affected products

The vulnerability affects the Microsoft Azure Kubernetes Service product, specifically the following versions:

- Versions prior to 0.3.3.
- From version 1.0.0 onwards, this one inclusive.

Solution

It is recommended to update to the latest version to fix errors.

This update will be performed by updating the confcom extension using the following command-line interface:

- `az extension update -n confcom`

References

- www.incibe.es
- www.msrc.microsoft.com

Patches

CRITICAL

New Security Patch for JetBrains TeamCity

Date: March 4, 2024
CVE: CVE-2024-27198 and 3 more

Description

JetBrains has released a series of security updates to address several issues affecting the TeamCity product. The update fixes a total of 4 vulnerabilities, one of them being critical, another one of high severity, and two others of medium severity.

The critical vulnerability (CVE-2024-27198) allows users to bypass the authentication process, thereby granting them unauthorized access to perform administrative actions. This security loophole enabled anyone to execute administrative tasks without the need for authentication.

The remaining vulnerabilities fixed are:

- CVE-2024-27199 (High): Path traversal vulnerability.
- CVE-2024-28173 (Medium): Vulnerability in password fields.
- CVE-2024-28174 (Medium): Incorrect authorization of S3 access URLs.

Affected products

This vulnerability affects the TeamCity product in versions prior to 2023.11.4. JetBrains organizes its versions based on the date, so it can be intuitively observed whether you have a version older than the required one.

Solution

JetBrains recommends updating to version 2023.11.4 of the product, which contains the necessary patches to mitigate the described vulnerabilities.

References

- nvd.nist.gov
- www.jetbrains.com

HIGH

New patches for Apple's operating systems

Date: March 5, 2024
CVE: CVE-2024-23225 and 1 more

Description

Apple has released emergency security updates that address two 0-day vulnerabilities in iOS, identified as CVE-2024-23225 and CVE-2024-23296, which were exploited in attacks targeting iPhone devices.

CVE-2024-23225 and CVE-2024-23296 are two memory corruption vulnerabilities affecting iOS and iPadOS operating systems. Exploiting these vulnerabilities would allow an attacker with arbitrary read and write capabilities in the kernel to bypass its memory protections.

Specifically, CVE-2024-23225 is a kernel memory corruption flaw, while CVE-2024-23296 is an RTKit memory corruption flaw.

Affected products

The vulnerabilities affect the following devices:

- iPhone XS and later.
- iPad Pro 12.9-inch 2nd generation and later.
- iPad Pro 10.5-inch.
- iPad Pro 11-inch 1st generation and later.
- iPad Air 3rd generation and later.
- iPad 6th generation and later.
- iPad mini 5th generation and later.

Solution

Apple recommends updating your devices to iOS 17.4, iPadOS 17.4, iOS 16.7.6, and iPadOS 16.7.6, addressing a memory corruption issue by improving validation.

References

- support.apple.com
- securityaffairs.com

Events

IV STIC CONFERENCE & ROOTED_CON CONGRESS (10 - 12 April)

The two leading events in the cybersecurity sector in Spain, the STIC Conference and the RootedCON Congress, have joined forces to jointly organise a new international chapter of their meetings, this time in Panama, from April 10 to 12, 2024. Both have chosen the Panamanian city as a strategic place to hold the largest cybersecurity event in Latin America.

Link

I CYBERLEGAL CONFERENCE (23 April)

Red Seguridad will hold the first Cyberlegal Conference at the Ilustre Colegio de la Abogacía de Madrid on April 23rd. An event of great novelty whose main objective is to gain firsthand knowledge of the challenges that cybersecurity imposes on both the Administration of Justice (judges, prosecutors...) and Law Enforcement Agencies as well as on professionals in the legal field (lawyers, solicitors, etc.) and the legal departments of organisations.

Link

ASLAN 2024 (17-18 abril)

The 31st edition of the Aslan Congress & Expo 2024 is already underway, under the slogan "A breakthrough in digitalisation". Organised by the @aslan association, the congress will explore artificial intelligence (AI) in the digital transformation processes of organisations. It will take place on 17 and 18 April 2024 at the IFEMA Municipal Conference Centre in Madrid.

Link

HACKER WORLD 2024 (22 April)

At Hacker World, more than 30 experts will address the different topics of relevance in the world of cybersecurity, in addition, attendees will have the opportunity not only to share knowledge and experiences, but also to promote networking.

Link

Resources

Kali Linux 2024.1
The most outstanding novelty of Kali Linux 2024.1 is not related to the operating system, but to the infrastructure, since the distribution has presented the CDN Micro Mirror, which is "a network of mirrors dedicated to serving Linux and Free Software. Unlike traditional mirrors that hold around 50TB of project files, Micro Mirrors are machines with 'only' a few terabytes of storage that focus on hosting only the most in-demand projects.
Link

SORA
OpenAI, the pioneer in generative artificial intelligence, has unveiled Sora, a revolutionary model that converts textual descriptions into realistic video scenes. Sora is capable of creating complex scenes with multiple characters and specific movements, including details of both the main component and the background. The model understands how objects interact in the physical world and generates compelling characters that express vibrant emotions.
Link

Cybersecurity Trends 2024
Learn about the most impactful Cybersecurity Trends for 2024 from various analysts such as Gartner, Google, Forrester, IDC, and SealPath. This article outlines predictions for the future and aims to help you fight cyber threats in 2024 and stay on top of the latest to improve your ability to respond and adapt.
Link

Cyber-Cluedo
The National Cryptologic Centre (CCN), attached to the National Intelligence Centre, has developed a new training tool to raise awareness about phishing. "Cyber-Cluedo" is now incorporated into the gamification section of "Angels". Its main objective is to promote learning about cybersecurity threats, identify the risks associated with identity theft, and implement the appropriate security measures for better protection against this type of attack.
Link

Powered by the cybersecurity NTT DATA team

es.nttdata.com