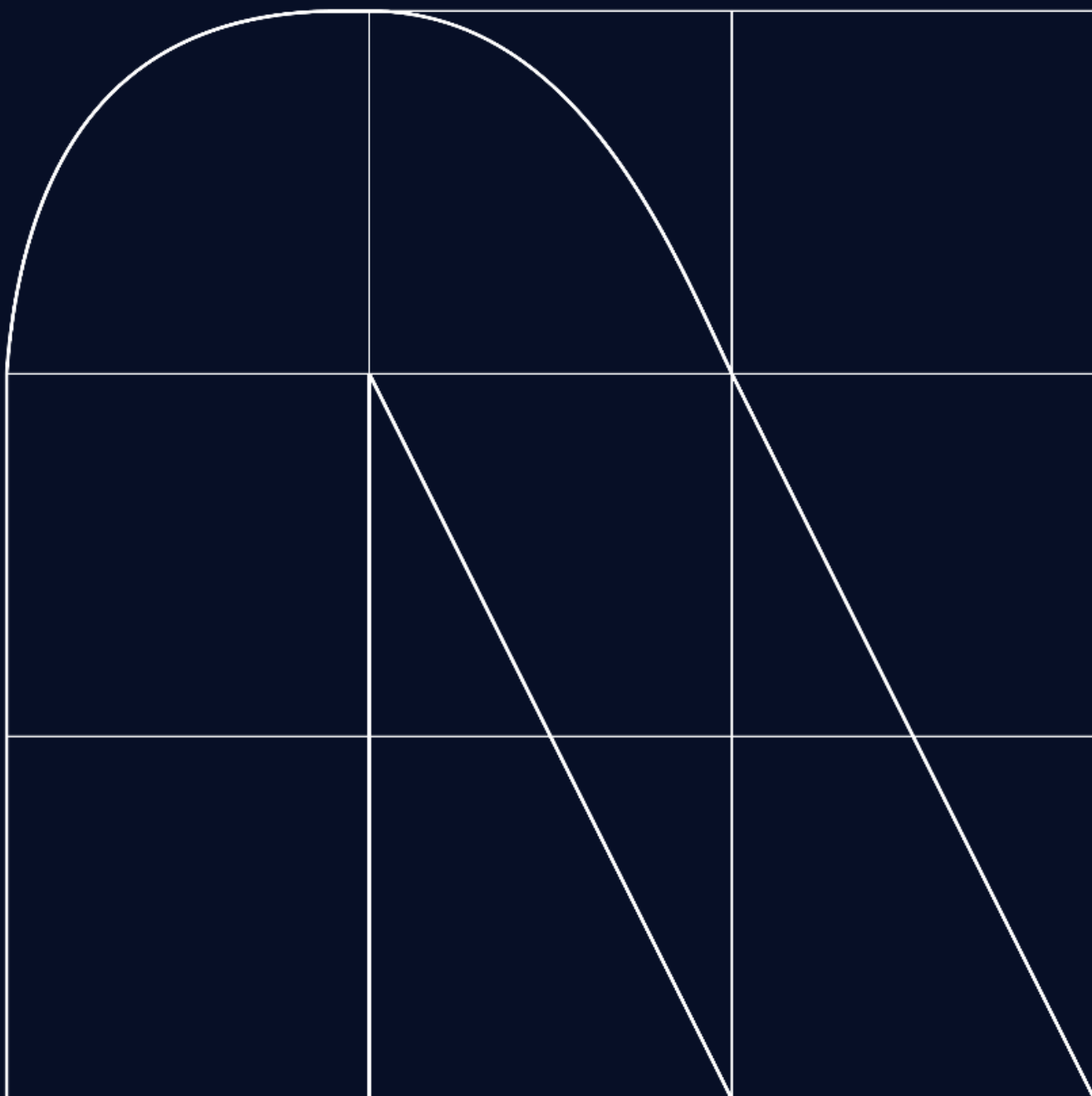
Issue 85 / December 2023

NTT DATA

Radar

Cybersecurity magazine



The long road to evolutionary cybersecurity

By: Conrad López

An organisation's information security policy determines, to a large extent, its information security objectives, which are associated with the organisation's mission, vision and values. Cybersecurity strategy is the instrument that allows the organisation's management to establish the path to follow in order to achieve these objectives over time, adapting to the changes that the company's own evolution undergoes in response to the needs and requirements determined by the changing environment in which it operates.

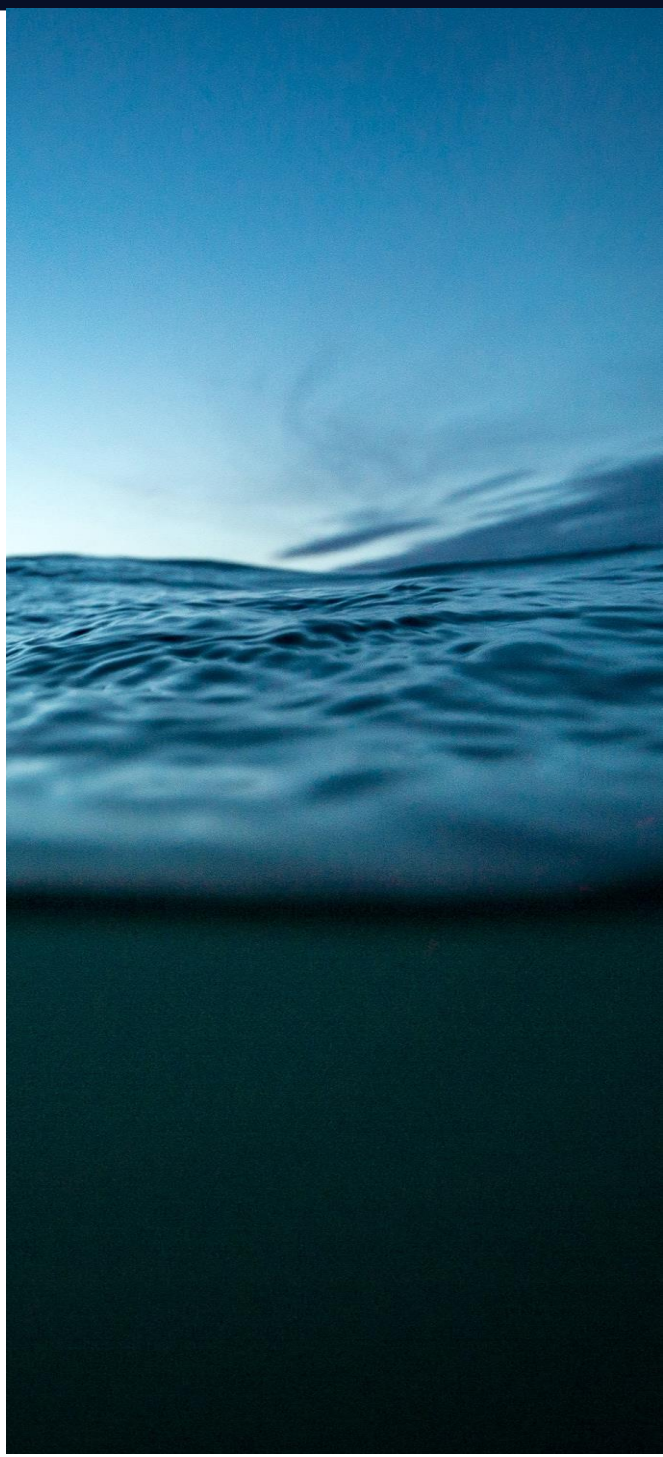
Aligning cybersecurity strategy with business strategy is an ongoing process that requires close collaboration between the cybersecurity function and the organisation's management. When this alignment is achieved, cybersecurity becomes an enabler of business objectives by protecting the assets and reputation of the organisation. But how do you achieve this strategic alignment? Some key factors are:

Understanding and involvement on the part of management: it is essential that business leaders understand the importance of cybersecurity and how it is intrinsically linked to their success. This can be achieved through specific awareness and training sessions for leaders. In short, the cybersecurity function should be involved in strategic planning to ensure that security risks and opportunities are taken into account.

Integration into business processes: cybersecurity must be naturally embedded in business processes so that it is an indispensable component of daily operations. This includes critical asset identification, risk management, secure supply chain management, project management and decision-making.

Technological and business risk assessment: it is not only about assessing technological risks, but also business risks. An adequate understanding of how cyber risks can impact on business continuity, company reputation and regulatory compliance is necessary. In any case, technological risk is an essential component of the operational risk of organisations in their digital transformation.

Effective communication: It is crucial to establish constant communication between the cybersecurity function and the organisation's management, keeping managers informed about cyber threats, vulnerabilities and risk mitigation achievements.



Aligned cybersecurity objectives: It is necessary to align cybersecurity objectives with the company's business development and technological evolution objectives. This requires an understanding and internalisation of many aspects, such as:

Identification of the risk scenario to which the organisation is subjected, developing an appropriate threat intelligence strategy and the necessary response, both proactively and reactively.

Regulatory implications and technological requirements imposed by the presence of the organisation in different geographical areas.

Compliance needs of the existing regulation in the market sector in which the organisation operates.

New security challenges imposed by the technological evolution planned for the organisation to support its business strategy.

Improvement of the organisation's cybersecurity culture, maintaining an adequate awareness of employees, collaborators and its management.

Correct measurement of the effectiveness of the cybersecurity management processes defined in the organisation's security governance model, facilitating decision-making to ensure alignment with the objectives set and facilitating, as far as possible, the evaluation of the return on investment in cybersecurity.

Resource allocation: It is necessary to align cybersecurity resources with business priorities. This may involve allocating budget and personnel according to the identified cybersecurity needs, and in particular facilitating the independence and capacity of the cybersecurity officer (CISO) in carrying out their role.

In addition, the constant evolution of the technological, social, commercial, political and business environment requires the ability to assess the organisation's security situation (situational awareness), flexibly adapting the cybersecurity strategy as threats and business objectives change. This requires regular evaluations (regulatory audits, technical audits, maturity analysis of the cybersecurity function, re-evaluations of the existing control framework, etc.) and adjusting the strategy as necessary.

These complex aspects require knowledge and dedication which, taking into account the results of multiple studies by analysts on the situation of cybersecurity in Spain, make it increasingly necessary for most organisations to have the support of expert collaborators in the field to help ensure the achievement of their objectives and their own cybersecurity strategy. Data such as the fact that the number of organisations with 5 or less employees dedicated to the cybersecurity function in Spain, regardless of the company's turnover, exceeds 50% (and, among them, 30% with turnover over €100M (ISMS Forum, III Cybersecurity Maturity Indicator) would seem to corroborate this statement.

Conrad López
Cybersecurity Technical Manager

Cyberchronicles: The complexity of managing sensitive information in the cyber-storm

By: NTT DATA Europe & Latam

In the digital information age, the security of data handling is a crucial challenge. We find ourselves in a scenario where the integrity and confidentiality of our personal information hangs in the balance, constantly threatened by cybercriminals.

In recent weeks, a well-known airline has found itself at the epicentre of cybersecurity news after leaving sensitive information of thousands of its customers in the hands of cybercriminals. The attack, discovered on October 10 of this same year, has led the airline to issue an urgent alert to its customers, asking them to cancel their credit cards as a preventive measure given the seriousness of the situation.

The organisation has not yet published the official number of people affected, but according to different media that have echoed the news, the number of affected customers is said to be more than 100,000. This is not the first time it has happened, as a few years ago, the AEPD (Spanish Data Protection Agency) fined them €600,000 for not applying the security measures required by law. The company has not provided further details, but according to cybersecurity experts, there is speculation that the theft of data, including some of the most sensitive data such as the CVV of the cards, has been carried out by other means.

This company has been PCI-DSS certified since 2020, which means that its company has passed different independent audits that certify that it uses its customers' sensitive information in an appropriate and secure way. So early indications point to a possible code injection called web skimming, where attackers take advantage of this modification in the airline's source code to send such sensitive information to an external server.

The cyber-attack underlines not only the importance of adopting robust security practices such as through certifications, but it is also essential that companies invest in the continuous training of their personnel, making sure that they are updated on the latest security threats and techniques.

The implementation of advanced technologies such as intrusion detection systems is also key, crucial tools that allow you to quickly identify and respond to possible threats. However, technology alone is not enough; constant awareness and proactive vigilance are essential.

The rapid evolution of cybercriminals' tactics demands a vigilant attitude on the part of organisations, which must be aware of emerging and continuously developing threats in order to adapt their security strategies accordingly.

Therefore, this incident underlines the importance of combining certifications, continuous training, advanced technologies and a proactive mindset to safeguard the integrity and trust of customer information.

> The rapid evolution of cybercriminals' tactics demands a vigilant attitude on the part of organisations

From DevOps to SecDevOps: Merging security and agility

ANALYSIS

DevOps: Development + Operations. Merging software development processes with those pertaining to the integration and deployment of such developments. It sounds difficult, and indeed it is. If we add cybersecurity to the equation, it gets even more complicated. From that point on, we move on to DevSecOps, or even SecDevOps, depending on how present security is in the whole process.

The synergies between cybersecurity and DevOps

DevOps. Initially DevOps arises from the need to build and deliver software continuously and automatically as quickly as possible. A team of developers finishes implementing a new functionality in a web application, and it is important that this functionality is tested, integrated and deployed as soon as possible in production environments in order to make it available to the end user as soon as possible.

The key concepts here are "collaboration" and "streamlining". We need to collaborate to achieve the agility in software delivery that we aspire to. This presents a number of challenges, most notably a change of mindset and that the need for communication between departments sometimes proves not to be easy. A developer would find it difficult to change the mindset to that of an operations role and vice versa. However, the change does not have to be immediate either and processes/technologies can be incorporated little by little.

Business concerns about cybersecurity have been growing in recent years, as both the number of attacks and the severity of the consequences have increased. It became clear that it was necessary to develop software with special attention to software security.

We have a scenario in which we need to build and deliver software in an agile way (DevOps), but at the same time guaranteeing its robustness against cyber-attacks (Sec). This is how DevSecOps was born. Again, this presents its challenges, as it is now not only a collaboration between Devs and Ops, but also integrates the cybersecurity team. In addition, the inclusion of security tools and processes at the end can have an impact on how quickly a development goes out to a productive environment. This is because including the necessary analysis to verify the safety of such a development may slow down the overall process, especially if false positive filtering needs to be included. However, we must decide what is important: either that the developments go out as quickly as possible to productive environments regardless of the vulnerabilities they may contain, or that, despite a slower deployment speed, our developments have a sufficient degree of security.

From theory to practice: tools to make development secure

Nowadays there is a wide range of tools that help us to provide security to the developments included in a DevSecOps environment. Depending on the type of task they carry out and the time at which they are executed, we can differentiate between the following types:

- SAST: Static Application Security Testing. In this classification we find those tools that analyse the source code of developments in search of possible defects that may cause security vulnerabilities. Examples of SAST technologies are Veracode, Fortify or Coverity.
- SCA: Software Composition Analysis. This type of software is responsible for detecting if there are known security vulnerabilities in the external dependencies used in the developments. Examples of SCA tools are Snyk, Black Duck or XRay.
- DAST: Dynamic Application Security Testing. Similar to SAST, but instead of analysing the source code of the developments, it analyses their behaviour once deployed. It automatically tests for behaviour that could lead to security breaches, such as information leaks or unavailability of services. Examples of DAST tools are Burp Suite, Nessus, Acunetix.
- RASP: Runtime application self-protection. Similar to the WAF (Web Application Firewall) technology. It is responsible for detecting and blocking possible attack attempts on deployed applications. Unlike WAFs, which operate at the network level, RASPs operate at the application level. They have certain information about the functionality and internal infrastructure of the applications they protect and are therefore more accurate in detecting potential attacks. Examples of RASPs are Imperva, Hdiv and OpenRASP.

DevSecOps vs SecDevOps

Today, the two terms are used interchangeably as synonyms and the difference is quite blurred. However, there are some nuances that set them apart.

- DevSecOps is a DevOps environment with security additions: SAST/SCA tools to analyse code and dependencies, perhaps a RASP to monitor and protect already deployed developments... In short, security exists in the DevOps environment as a necessary addition, but without affecting each and every one of the processes that are executed.
- SecDevOps is a DevOps environment in which security is prioritised and a conscious focus is placed on ensuring that every existing process is carried out with security in mind. Developers have SAST analysis tools available in their IDEs; there is a regularly updated security test suite that is run every time code is uploaded to the repositories; full SAST, SCA, DAST and/or IAST analysis is run with security gates that prevent vulnerable developments from being deployed; and deployed developments are monitored and protected by RASP and/or SIEM tools.

While in DevSecOps security is contemplated and taken into account, in SecDevOps it is prioritised and considered the element that has to encompass the rest.

As a final note, our goal is to build software not only in an agile way, but also with the highest possible security guarantees. Therefore, we should always aim to have a SecDevOps environment. However, trying to move directly from a DevOps to a SecDevOps environment is likely to be counterproductive, as all users involved will be overwhelmed by the sheer volume of new tools and processes. The best strategy will be to gradually implement these tools and, at the same time, train users in the use of them.

Miguel Otero
Cybersecurity Lead Architect
NTT DATA Europe & Latam

Antonio Gallego
Cybersecurity Analyst
NTT DATA Europe & Latam

SBOM in Cybersecurity: The key to an effective defense.

TRENDS

With the growing threat of sophisticated cyber-attacks, organisations are constantly looking for innovative ways to protect their digital assets. In this context, the SBOM (Software Bill of Materials) emerges as a crucial tool for strengthening cyber defences.

The SBOM is essentially a detailed list of all the software components used in an application or system. This list provides vital information about the libraries, frameworks and modules that make up the software. In the context of cybersecurity, the SBOM becomes an invaluable tool, as it provides a complete overview of the potential attack surface.

By incorporating SBOM into the cybersecurity strategy, organisations gain unprecedented transparency in their software supply chain. This means that every component used in software development is documented and can be easily tracked.

Visibility in the supply chain is crucial to identify potential vulnerabilities and security risks. The ability to know and understand each element of software used allows organisations to take proactive measures to mitigate risks and strengthen their defences. One of the greatest benefits of the SBOM in the field of cybersecurity is its ability to facilitate the management of vulnerabilities and patches. By knowing all the software components and their versions, organizations can quickly identify known vulnerabilities and apply the corresponding patches efficiently.

This rapid response capability is essential to counter emerging threats. Cybercriminals often take advantage of known vulnerabilities in outdated software to carry out attacks. The SBOM allows organisations to close these security breaches in a timely manner, significantly reducing the risk of exploitation.

In a regulated environment, the SBOM becomes a key ally to ensure regulatory compliance. Increasingly stringent cybersecurity regulations require a proactive approach to managing risks. The SBOM provides detailed documentation that facilitates the demonstration of compliance with current regulations.

It also facilitates security audits. Security teams can thoroughly review the list of software components, verify the presence of patches, and assess the overall security posture of the organisation. This not only meets regulatory requirements, but also strengthens the organisation's security posture.

The incorporation of the SBOM in the safe development practices is essential to maximise its effectiveness. Integrating the SBOM into the software development lifecycle from the very beginning ensures that transparency and risk management are an integral part of the entire process.
Development teams can use the SBOM to make informed decisions about the selection of software components, evaluating the security of each element before its implementation.

This proactive practice contributes to the creation of more secure software from the very beginning, reducing the need for costly fixes at later stages.

In short, the SBOM has become an essential tool in modern cybersecurity. It provides transparency, visibility and efficiency in vulnerability management, which is crucial in an increasingly threatening digital environment. Integrating the SBOM into the cybersecurity strategy not only strengthens an organisation's defences, but also contributes to regulatory compliance and secure software development.

Ultimately, the SBOM is not simply a list of software components, but a strategic tool to build a more secure digital future.

Vulnerabilities

Vulnerability in Confluence Data Center and Server

Date: October 31, 2023
CVE: CVE-2023-22518

CRITICAL

CVSS: 10

Description

Atlassian has published a vulnerability of critical severity that affects its Confluence Data Center and Confluence Data Server products. This vulnerability affects all versions of both products.

Through this security flaw, an unauthenticated attacker could benefit from an incorrect authorisation, which could allow them to restart the Confluence instance and create an administrator account.

Once the administrator privileges have been obtained, the attacker could perform all kinds of actions on the Confluence instance, which means a complete loss of confidentiality, integrity and availability.

Links:
https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html
https://jira.atlassian.com/browse/CONFSERVER-93142
https://nvd.nist.gov/vuln/detail/CVE-2023-22518

Affected products:
This vulnerability affects all versions of the following products:

- Confluence Data Center
- Confluence Data Server

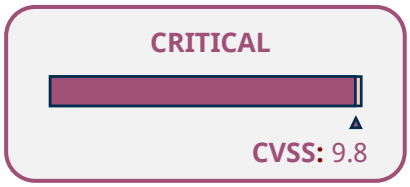
Solution:
The manufacturer has recommended to update to one of the following versions as soon as possible:

- 7.19.16
- 8.3.4
- 8.4.4
- 8.5.3
- 8.6.1

Vulnerabilities

Multiple vulnerabilities in QNAP products

Date: November 3, 2023
CVE: CVE-2023-23368



Description

On November 4, QNAP published a critical vulnerability that affects several of its products (QTS, QuTS hero and QuTScloud).

This command injection vulnerability could allow attackers to execute commands remotely.

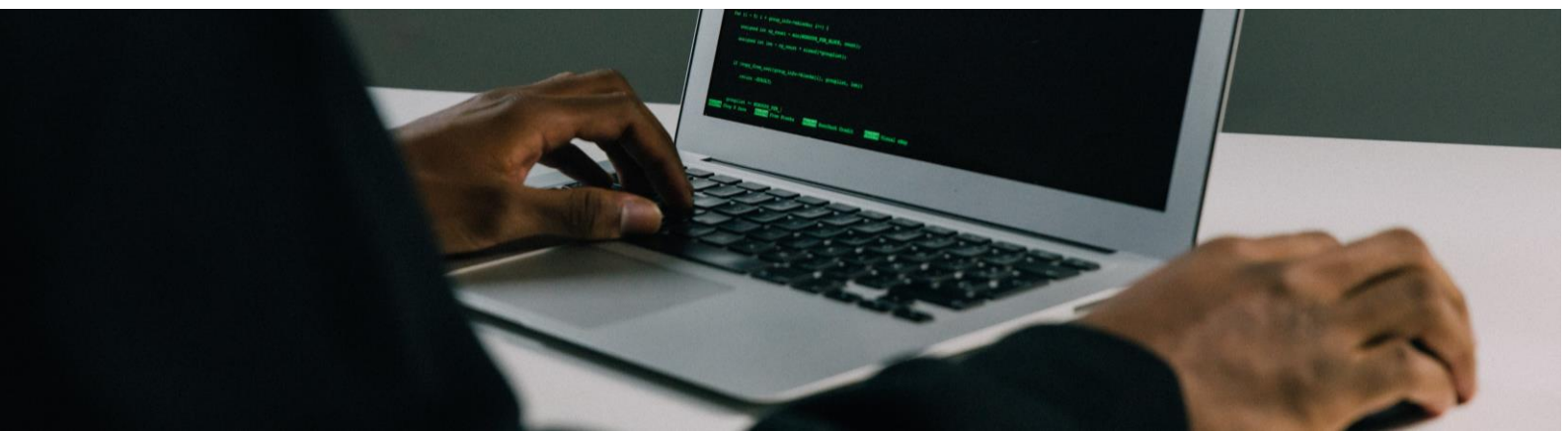
QNAP has reported that the problem has been solved and that it is recommended to update the systems to the latest version as soon as possible to avoid the exploitation of this vulnerability by external attackers.

Links:
https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-23368
https://www.qnap.com/en/security-advisory/qsa-23-31
https://nvd.nist.gov/vuln/detail/CVE-2023-23368

Affected products:
The different products affected by the vulnerability are as follows:

- QTS (versions 5.0.x)
- QTS (versions 4.5.x)
- QuTS hero (versions h5.0.x)
- QuTS hero (versions h4.5.x)
- QuTScloud (versions c5.0.x)

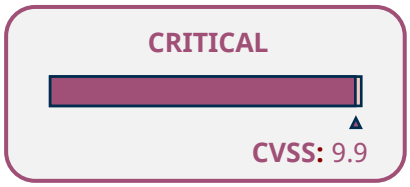
Solution:
The manufacturer has published a series of updates in order to patch this vulnerability. It is recommended to install such patches as soon as possible.



Patches

Multiple patches for vulnerabilities in Veeam

Date: November 6, 2023
CVEs: CVE-2023-38547, CVE-2023-38548, CVE-2023-38549 and CVE-2023-41723



Description

Veeam has published a series of security patches that fix a total of 4 vulnerabilities, two of them of critical severity and two others of medium severity:

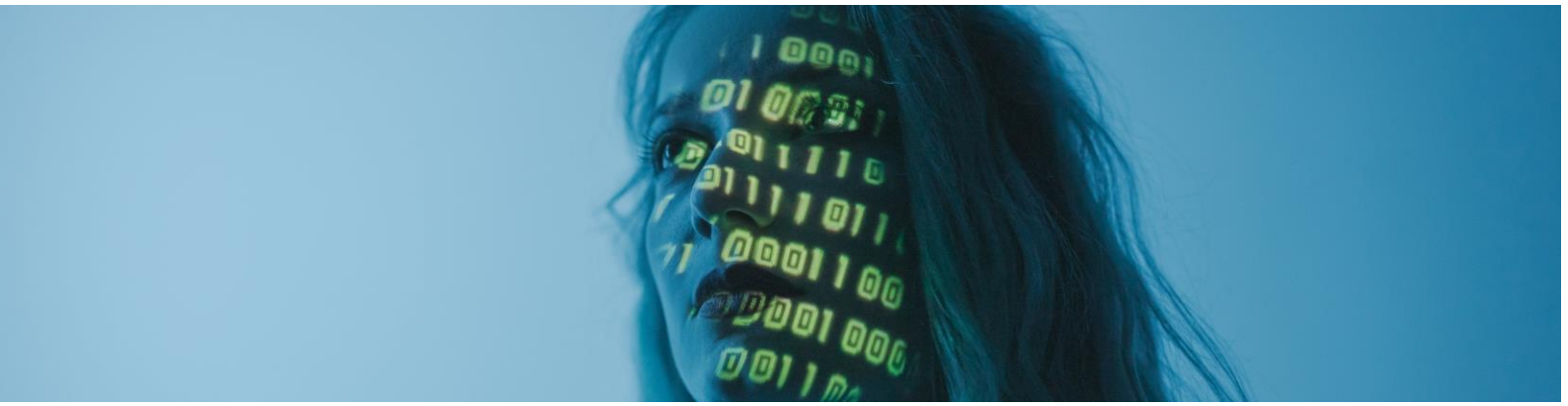
- **CVE-2023-38547**: a critical vulnerability that allows an unauthenticated attacker to remotely execute code on SQL servers.
- **CVE-2023-38548**: Critical severity vulnerability that would allow an unprivileged user with access to Veeam ONE Web Client to obtain NTLM *hashes* of accounts used by Veeam.
- **CVE-2023-38549:** medium severity XSS vulnerability that allows the escalation of user privileges from "Power User" to "Administrator".
- **CVE-2023-41723**: medium severity vulnerability that allows a user with "Read-Only" privileges to consult information from the "Dashboard Schedule" section.

Veeam has recommended to immediately stop the Veeam ONE services in case of using affected versions, apply the patches and restart said services.

Links:
https://www.veeam.com/kb4508
https://thehackernews.com/2023/11/critical-flaws-discovered-in-veeam-one.html

Affected products:
These vulnerabilities affect the following versions of Veeam ONE:
- Veeam ONE 11
- Veeam ONE 11a
- Veeam ONE 12

Update:
The solution proposed by the manufacturer consists of updating to the following versions:
- Veeam ONE 11 (11.0.0.1379)
- Veeam ONE 11a (11.0.1.1880)
- Veeam ONE 12 P20230314 (12.0.1.2591)



Patches

Multiple security patches for Microsoft products

Date: November 14, 2023
CVEs: CVE-2023-36025, CVE-2023-36033, CVE-2023-36036, CVE-2023-36038, CVE-2023-36413, CVE-2023-36028, CVE-2023-36397

CRITICAL

CVSS: 9.8

Description

Microsoft has published its monthly security bulletin to fix a total of 63 vulnerabilities in its products. Among them, there are a total of 5 0-day vulnerabilities:

- **CVE-2023-36025 (CVSS: 8.8):** vulnerability in Windows SmartScreen Security Feature that allows to evade some security measures.
- **CVE-2023-36033 (CVSS: 7.8):** elevation of privilege vulnerability in Windows DWM Core Library.
- **CVE-2023-36036 (CVSS: 7.8):** privilege escalation vulnerability in Windows Cloud Files Mini Filter Driver.
- **CVE-2023-36038 (CVSS: 8.2):** DoS vulnerability in ASP.NET Core.
- **CVE-2023-36413 (CVSS: 6.5):** vulnerability in Microsoft Office that allows to evade certain security features.

In addition, two critical severity vulnerabilities have been fixed:

- **CVE-2023-36028 (CVSS: 9.8):** remote code execution vulnerability in Microsoft Protected Extensible Protocol (PEAP).
- **CVE-2023-36397 (CVSS: 9.8):** remote code execution vulnerability in Windows Pragmatic General Multicast (PGM).

Microsoft recommends the installation of all security patches on the affected products, as some of them are being actively exploited.

Links:
https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov
https://thehackernews.com/2023/11/alert-microsoft-releases-patch-updates.html

Affected products:
These vulnerabilities cover a large number of Microsoft products. These products can be consulted in:
https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov

Update:
Apply the corresponding security patch on the affected products.

Events

XV STIC CCN-CERT CONFERENCE
30 November – 3 December

The STIC CCN-CERT Conference, in its fifteenth edition from November 30 to December 3, is a key cybersecurity event in Spain that has evolved over fifteen years, bringing together professionals, public entities, companies and universities. Despite the challenges of COVID-19, the latest edition was successfully adapted. This year, under the theme "Cybersecurity 360º. Identity and Data Control", the event will be hybrid, with face-to-face and online activities, offering a comprehensive view of the sector at national and international level

Link

THE LAST SUPPER OF OSINT
2 December

In response to the growing importance of cyberspace and cybersecurity in global geopolitics, QuantiKa14 is organising a unique ephemeral event: The Last OSINT Supper in Seville. This exceptional meeting will offer cutting-edge discussions on cyber intelligence, with distinguished speakers and sponsors. The evening will include three presentations, a coffee break and networking, followed by a dinner where the conversation will be as delicious as the dishes. Seville will become the epicentre of this vital conversation at a crucial time to stay informed and connected in this key area.

Link

BLACK HAT EUROPE 2023
4 - 7 December

Black Hat is a leading IT security event that brings together industry experts to explore the latest research and trends. For four days, it offers practical technical trainings followed by two days of presentations on vulnerabilities. Black Hat Europe will be face-to-face in London from 4-7 December, followed by a virtual experience from 13 December with recordings of all sessions. This year, the "Certified Pentester" program is introduced, a one-day practical exam focused on pentesting.

Link

CIBER1C MX
7 December

Ciberilatam, in collaboration with the National Cryptological Center of Spain and the Borredá Foundation, organises the I Congress of Cybersecurity in Critical Infrastructures and Essential Services of Mexico (CIBER1C MX) on December 7 at the *Club de los Periodistas*. This event, also supported by Segurilatam, will bring together professionals to explore cybersecurity strategies in the protection of critical infrastructures and essential government services, addressing challenges, threats in cybersecurity for corporate governance and discussing the future of the sector, among other relevant topics.

Link

Resources

Flipper zero challenges the security of iPhones

The Flipper Zero, known as the "tamagotchi" for hackers, has gained notoriety for its versatility and ability to perform hacking experiments. It has recently been revealed that this multifunctional device can challenge the security of iPhones, in particular those running iOS 17. Priced at about 250 euros, the Flipper Zero can intercept and play back wireless signals, but its ability to send iPhones into denial-of-service (DoS) loops by a flood of messages via Bluetooth has raised significant concerns. While there is still no definitive solution to prevent these attacks, the situation highlights the importance of regulation and ethics in the field of cybersecurity as technologies advance and are used maliciously.

Link

Microsoft offers new AI tools to deal with cyber attacks

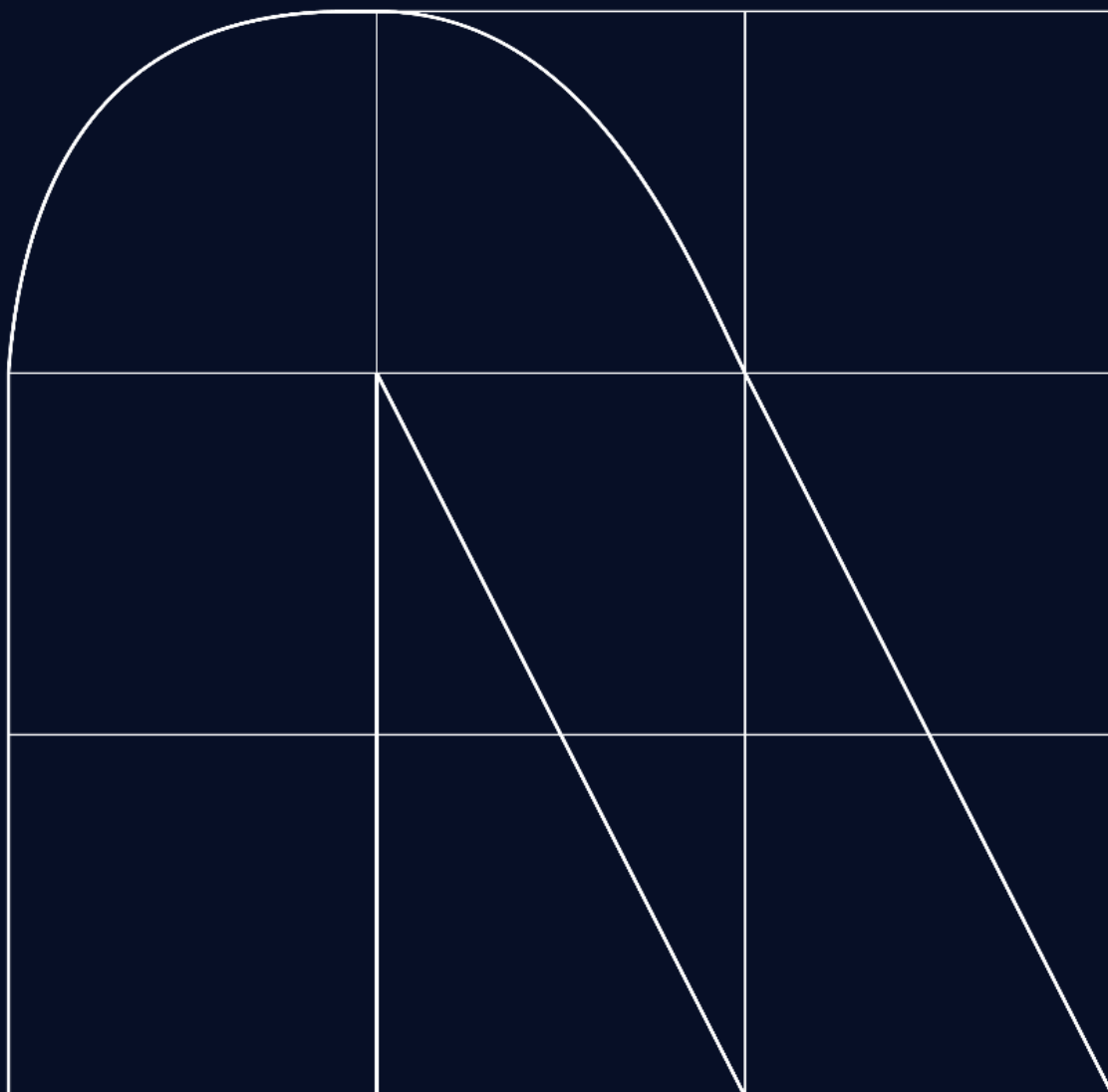
Microsoft has announced its commitment to improve in the field of cybersecurity, expanding the capabilities of its tools and techniques to detect threats. The company plans to make these capabilities directly available to its customers by providing them with artificial intelligence (AI) tools with the aim of strengthening the defence against cyber-attacks. This approach reflects Microsoft's initiative to empower users with advanced solutions in the fight against digital threats.

Link

The fake son scam (whatsapp, bizum...)

The National Police has issued a warning to citizens about the fake son scam, which has led to the arrest of 17 people in Catalonia for swindling 60,000 euros with this method. The scam involves scammers posing as sons or daughters through WhatsApp messages, requesting money for fictitious emergencies. The victims, usually worried mothers, transfer money to bank accounts or Bizum IDs provided by the scammers. The police advise to be wary of unexpected messages, verify the authenticity of urgent money requests, contact the allegedly affected relatives directly and refrain from making transfers to unknown accounts to avoid falling into this type of scam

Link



Powered by the cybersecurity NTT DATA team

es.nttdata.com