NUMBER 64 | MARCH 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

WHY DEPENDENCIES ARE NOT THIRD-PARTY

It is becoming easier and easier to access sources of knowledge, to learn about the functioning of new technologies and to become aware of application architectures. It is as easy as accessing countless tutorials available on the Web. This is sensational, as it allows technology to make impressive progress in a short time, but at the same time, it also affects the number of potential attackers, users who take advantage of their extensive knowledge of technology to jeopardise the security of organisations by exploiting existing weaknesses in the software they generate.

This scenario is something that companies are well aware of and that is why the level of awareness on the need to secure software from the outset is improving considerably.

The further left in the build flow (from left to right, from start to finish of a development process), the easier and less costly it is to apply protective measures on the software. For this reason, organisations are increasingly incorporating security controls in the early stages of their secure software development lifecycle (S-SDLC).

One of the most important security controls carried out in these initial stages is the security analysis of the dependencies or libraries used in the software. Recently, there has been a very important milestone in terms of exploitation of vulnerable libraries: the well-known incident involving the Apache Log4J library in mid-December 2021. Software developers all over the world almost had a nervous breakdown due to the numerous library changes they had to make in a short period of time.

The appearance of CVEs on the dependencies and libraries used by a software is something that no organisation can avoid; however, there are methods to detect whether a dependency/library is vulnerable as quickly as possible, and even to block the publication in production environments of software with vulnerable dependencies: Dependency analysers are the tools applied for this purpose.

Many library repositories already incorporate such modules, allowing libraries to be analysed recursively and periodically, preventing any developer from using a vulnerable library when building their software. For this reason, it is very important for organisations to have their own library and dependency repositories, where only secure libraries are stored, and also to ensure their security in the future, in case new CVEs are discovered over time.

For this quest for dependency security to take effect, it is very important that development teams are aware that they should only use libraries from trusted company repositories and under no circumstances use public repositories of libraries, the provenance of which may be very dubious.

In our experience, the level of security maturity in the S-SDLC of companies is increasing, because, as we mentioned at the beginning, organisations are becoming increasingly aware of the need to protect themselves. However, there is still a long way to go, as in all likelihood, a large part of organisations' software has libraries with CVEs; even more so, there are probably organisations whose software contains some version of the Log4J libraries with vulnerabilities, and if you do not believe us…

Would you be able to say how many vulnerabilities in different versions of Log4J came to light by the end of 2021?

Jose Carlos Moral

Technical Manager. Security Architecture at NTT Data Spain

CYBER NEWS

We open this month's cyber chronicle with one of the most frequent cyber-attacks in recent months: ransomware.

2021 was the year in which ransomware attacks exploded, making it the attack of choice for criminals, and there is every indication that it will continue to grow in strength and will be just as prevalent in early 2022. As an example of this, one of the latest types of ransomware to come to light at the end of January was DeadBolt, which exploited a 0-day vulnerability in NAS (Network Attached Storage) devices from vendor QNAP Systems Inc. and demanded a ransom of 0.03 Bitcoins from its victims to recover their encrypted data, while offering QNAP the possibility to provide details of the discovered vulnerability in exchange for 5 Bitcoins, or approximately 171,000 Euros.

> "New malware campaign distributed via the Windows update service launched by the North Korean Lazarus group".

This vulnerability, which allowed arbitrary code to be executed remotely, was classified as critical and has been mitigated in the latest versions of QTS or QuTS released by QNAP.

It has also recently been reported that multiple European ports in the Netherlands and Belgium are victims of a type of ransomware attack affecting the oil supply chain. This attack has paralysed ports such as Amsterdam-Rotterdam-Antwerp, forcing the affected oil companies to invoke the legal clause of declaring "force majeure" for not being able to fulfil their contractual obligations.

As everything comes in threes, another victim of this type of attack has been the British company KP Snacks, which has caused several companies dependent on its supplies to run out of stock. Behind this attack is the criminal group Conti, who have claimed responsibility for it, as well as a payment for the recovery of the encrypted files from KP Snacks.

Another relevant news item of this period was the new malware campaign distributed via the Windows update service launched by the North Korean Lazarus group. The group, also known as APT38, managed to load a malicious binary (drops_Ink.dll) inside one of the Windows update packages (wuauclt.exe) so that when the victim downloaded the legitimate package from the Windows Update service, the malicious DLL (wuaueng.dll) was executed undetected in the background. This DLL allowed the Lazarus group to establish communication between the infected system and a C2 server that distributed more malware from a GitHub repository created in mid-January.

On the other hand, in Spain and Germany, the banking Trojan FluBot has gained prominence. This malware, which affects Android devices, hides in the device, and gains full control of it, seeking to steal financial data, SMS contacts and any other type of private information on the device. It is mainly distributed through social engineering, impersonating important companies, and using an SMS from parcel delivery companies as a typical lure.

Another type of malware that made headlines this month was the Vultur Stealer Trojan, which was hidden inside the 2FA Authenticator app, available on Google Play for several weeks without being detected, and which was downloaded more than 10,000 times. The rogue app, which requested multiple permissions in order to be used, collected user data, especially location, credentials, and financial information, and could even make changes to the system, such as disabling the screen lock or password and downloading and installing other apps, among other things.

On a different note, the cloud and its benefits are enormous in terms of data maintenance and persistence. However, its use must be accompanied by a correct data processing and configuration policy, and it can be a double-edged sword if it is not configured properly, as has recently happened to the security of some airports located in South America. Due to a misconfiguration of Amazon Web Services' Bucket S3, which had its authentication system disabled, the information it contained was exposed on the Internet, causing a serious data breach of airport security personnel. This information contained, among other things, ID cards with staff data, employee photos and luggage.

And since we are talking about authentication problems, we find that more and more phishing kits are being developed that seek, as their main objective, to bypass two-factor authentication (MFA). Typically, these kits seek to steal tokens through man-in-the-middle (MiTM) attacks, so there has recently been an increase in the number of kits that implement an attack based on the use of a transparent reverse proxy (TRP), allowing the attacker to intercept an existing legitimate session in the browser and collect information as it appears on the screen, thus avoiding the classic attacks that consisted of creating clones of the target pages. This allows attackers to obtain browsing data such as cookies or authentication tokens that can be used to impersonate the victim. While this is not a new attack, it is gaining popularity thanks to the increased use of 2FA.

Moving on, 15 vulnerabilities on CISCO routers have recently been published. The three most severe vulnerabilities (CVE-2022-20699, CVE-2022-20700 and CVE-2022-20707), were rated 10.0 (CRITICAL), as they allowed elevation of privileges and execution of arbitrary code on Small Business RV160, RV260, RV340 and RV345 series routers. CISCO has patched all found flaws and urges all customers to upgrade to the latest software version as soon as possible, as public proof-of-concepts are known to exist for the exploitation of many of them.

Finally, the US Cybersecurity and Infrastructure Security Agency (CISA) is urging federal agencies to protect their systems from an actively exploited vulnerability in Windows systems. This corresponds to CVE-2022-21882 and has a risk score of 7.0 (HIGH), as it is an elevation of privilege vulnerability affecting the Win32k component.

CYBER-SURVEILLANCE AGAINST NEW THREATS

By: NTT DATA

We live in an information society in which, both in the workplace and outside it, we are constantly sharing information of different kinds, whether it be simple documents, publishing content or simply signing up to a website. This set of actions requires a certain amount of care on our part, as we may be exposing more information than necessary, or we may not be doing so in the most secure way.

All this information related to us, and our company makes up the digital footprint that we leave in cyberspace, which can be collected by malicious users in order to carry out actions that jeopardise the confidentiality, integrity, and availability of the data.

Therefore, in order to mitigate these possible risks related to information, the term Cyber-surveillance appears.

Cyber-surveillance refers to the monitoring of all computer activity carried out by a person or company, whether connected to the internet or not. The purpose of this practice is to avoid possible risks produced by the correct or incorrect use of connected devices, such as information leaks, phishing, or vulnerabilities, among others.

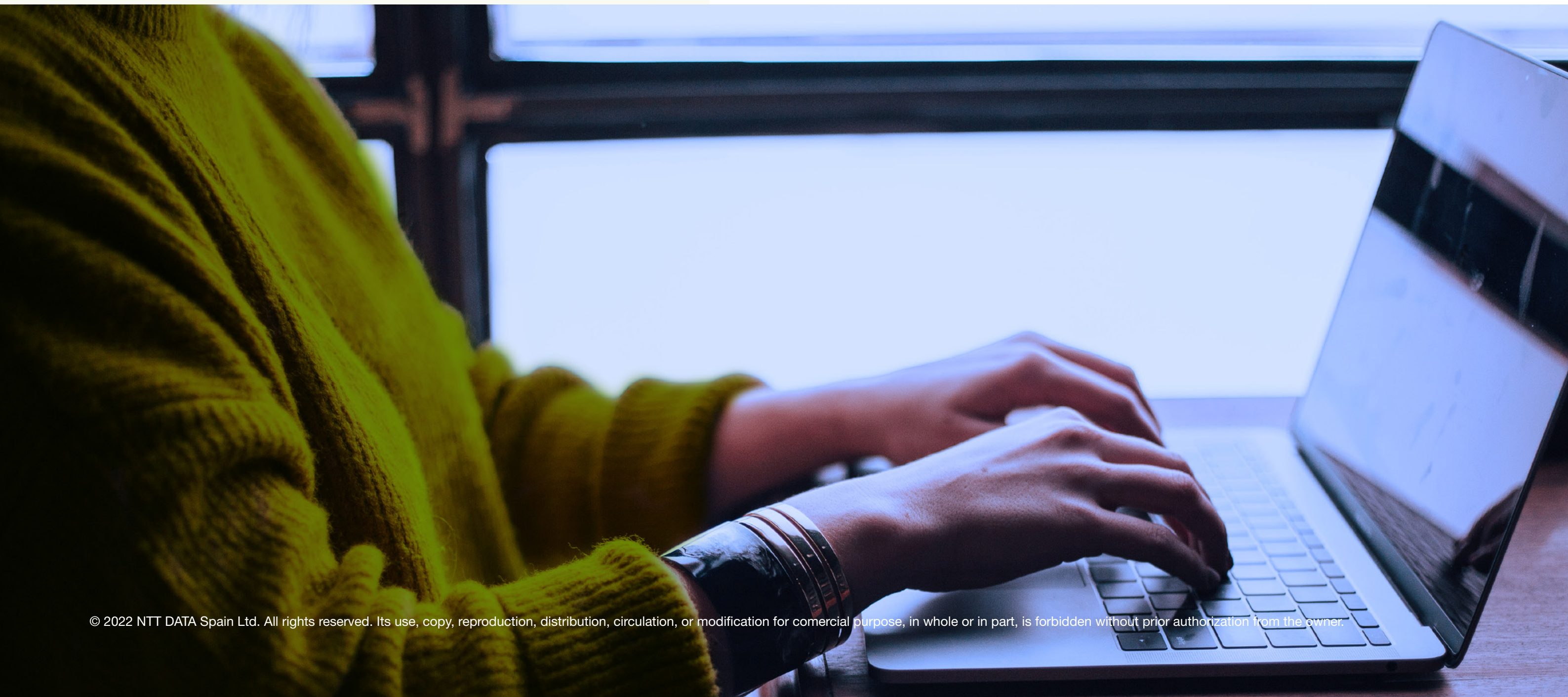
Some of the monitoring options present in cyber-surveillance tasks are detailed below.

Information Leakage

Normally, a data leak is caused by an improper publication in a public environment, a server configuration failure or simply the compromise of the systems that safeguard the information. To do so, we try to detect confidential documents, emails, source code, private files or other sensitive information belonging to an individual and/or company that is accessible both on the Surface Web and on the Deep/Dark Web.

Credential Leakage

Another point to bear in mind is the leakage of credentials. As employees, we are often unaware of where we log in with our corporate email, and not only that, but we even provide the corporate password. For this reason, detection of published corporate credentials is carried out thanks to different sources of information and databases.



Defacement

The cyber-attack known as "defacement", perhaps not very well known, but which causes great economic losses, as well as a company's bad reputation and image, thus compromising its policy. This type of attack consists of changing the legitimate appearance of a website. For early detection, it is necessary to monitor the content of the clients' websites.

Phishing

To deal with possible phishing attacks, which are carried out anonymously, for a low cost and effort, phishing detection and alerts are carried out, including support in mitigating them. To this end, both original domains and other similar domains that could be used by an attacker are monitored.

Carding

With regard to combating carding, known as the illegitimate use of stolen credit cards for financial gain, hidden markets where these cards are sold at a very low cost are uncovered. The aim is to detect the theft of credit cards, bank accounts, etc., that may be associated with customers in order to prevent unauthorised use of these cards from having an impact on both image and expenses associated with bank fraud.

Public Vulnerabilities

Vulnerabilities are flaws, defects, or weaknesses in information systems, which can become an entry vector for attackers to carry out malicious actions that put these systems and their information at risk. To prevent this from happening, customers are notified of public vulnerabilities, as well as those discovered by scanning teams or published 0-days.

Domain Monitoring

The most visible part of a company are the domains, which are the first point of contact of customers, employees, etc. with the company. It is usually one of the most attacked points, so it is necessary to maximise the security of these assets to avoid identity theft or changes of registrar, among others. It is therefore important to control the domain logs that are used to avoid this type of attack.

Hacktivism

Hacktivists aim to break a computer system in order to extract information that they can use to promote ideological or humanitarian motives, usually advocating the removal of secrets or the disabling of services. These movements are developed and organised in private forums and social networks, creating global campaigns against local entities and statutes. It is difficult to penetrate these circles but monitoring social networks and certain forums helps to detect these acts.

Fraud

Impersonating a corporate application in the Android or IOS market place by imitating a company logo is just one of the techniques used by cybercriminals to spread fraudulent Malware or Adware, or to obtain customer information for further attacks. It is important to keep an eye on app markets, as well as possible publications on behalf of the company that may be suspected of fraud.

Reputation

Online reputation is the "image" that a person, company, brand, or institution projects on the Internet. The image does not only take into account what we express on social networks, but also the comments, opinions and news that are expressed by our target audience through the media, such as social networks. In this way, it is not only important what is communicated but also how it is perceived and what opinion the recipients have. Therefore, it is important to monitor the main social networks: Twitter, Facebook, Instagram, Google+, YouTube, LinkedIn..., as well as forums and websites where the client has a presence or where information related to the client has been published.

All of the above options, among many others, seek to detect the different threats that may arise, providing early warning and solutions to prevent possible attacks that may cause economic losses, bad reputation, and image, and even loss of customers, among others.

NTT DATA offers a Cyber-surveillance service in a 24x5 environment, which consists of several phases. Firstly, information is collected, which is then classified and filtered. Once false positives have been ruled out, the resulting information is carefully analysed to provide useful data in the form of a report to the end client.

TRENDS

Honeypots, Breadcrumbs and Deception techniques: Traps for cyber-criminals

Today, these terms are increasingly being used in the cybersecurity and cyberdefence sector, especially in those corporations that have a high level of cybersecurity maturity. But what exactly do these terms mean?

Among the most well-known Deception techniques are Honeypots. A Honeypot is a “trap” or “decoy” system located in a network or computer system whose purpose is to detect and prevent a possible attack on a computer system. It can be physical, such as a computer integrated in the system and its only function is to be this controlled trap, or a virtual and dynamic one deployed on the server that is only activated when necessary, saving resources and adapting it to the attacker.

Today’s honeypots are really powerful and allow us to “simulate” the real behaviour of a system or even a corporate subnetwork, making the cyber-attackers believe that they have entered a real system and that it is easy to take control. However, they will be on an isolated system where we will be able to see exactly what they are doing and what vulnerabilities they are trying to exploit.

Thanks to this technology, in addition to mitigating a possible cyber-attack, we will be able to analyse the profiles and intentions of the attackers by assessing aspects such as::

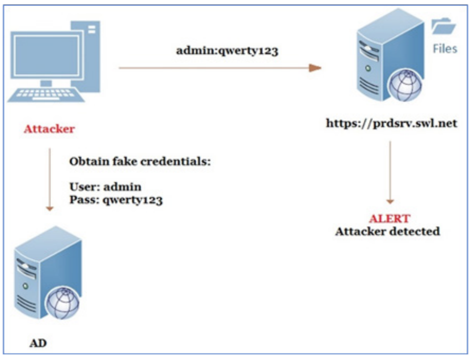
- Where the cybercriminals are coming from
- What modus operandi they are using
- What data or applications they are interested in
- The effectiveness of the security measures deployed in the company

There are mainly two types of Honeypots:

- Low interaction: Their interaction is almost null, and their functionality is limited to mimic applications or other systems or equipment in the network. For example: HoneyC (Client), Honeyd (Server).
- High interaction: They are usually equipment with real systems that have the same services that real servers would have. For example: Capture-HPC (Client), Argus (Server).

In addition to a Honeypot, what are known as BreadCrumbs are often used. This type of technique consists of intentionally leaving small decoys in a system or network, so that if they are found by an attacker, they can be used to continue their movement through the network.

A simple example of this type of technique would be as follows:



In the image above you can see how the attacker obtains fake credentials in clear text from the Active Directory (AD). These credentials will be used by the attacker to make a lateral move on other systems in the network which, upon detecting the access attempt, will set off alarms.

Although such systems can improve the security of an organisation, it is important to note that they must be used in conjunction with other security systems, as they do not detect all network activity but only that which is directed at them.

VULNERABILITIES

SAP

CVE-2022-22536, CVE-2022-22532, CVE-2022-22533

Date: 08/02/2022

Description. SAP's security team has released several security updates for different products that fix critical vulnerabilities. Among them are three affecting SAP Internet Communication Manager. Through their exploitation, affected organisations could suffer from theft of sensitive information, disruption of business-critical activities or ransomware attacks.

Link: https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022 (SAP)

https://onapsis.com/icmad-sap-cybersecurity-vulnerabilities?utm_campaign=2022-Q1-global-ICM-campaign-page&utm_medium=website&utm_source=third-party&utm_content=CISA-alert (Onapsis)

Affected Products.

The following are some of the versions and systems affected:

- SAP Web Dispatcher, Versions - 7.49, 7.53, 7.77, 7.81, 7.85, 7.22EXT, 7.86, 7.87
- SAP Content Server, Version - 7.53 Ubuntu 16.04 ESM (Xenial Xerus)
- SAP NetWeaver and ABAP Platform, Versions - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49
- SAP NetWeaver Application Server Java, Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53

Solution: Follow the recommendations given in the following link:

https://www.cisa.gov/uscert/ncas/current-activity/2022/02/08/critical-vulnerabilities-affecting-sap-applications-employing

Cisco

CVE-2022-20704,-20705,-20706,-20709,-20710,-20711,-20712

Date: 03/02/2022

Description. Multiple vulnerabilities have been published in Cisco products, some of them of critical severity. By exploiting them, an attacker could execute arbitrary code, unauthorised commands, unauthorised software, perform a denial of service and/or achieve privilege escalation. One of the critical vulnerabilities consists of a security flaw in the SSL VPN module of Cisco Small Business routers. It has also been detected that due to insufficient authentication mechanisms in the web-based management interface, an attacker could obtain root privileges

Link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-mult-vuln-KA9PK6D

https://es-la.tenable.com/blog/cve-2022-20699-cve-2022-20700-cve-2022-20708-critical-flaws-in-cisco-small-business-rv-series

Affected Products.

The vulnerabilities affect the following products:

- RV160 VPN Routers
- RV160W Wireless-AC VPN Routers
- RV260 VPN Routers
- RV260P VPN Routers with PoE
- RV260W Wireless-AC VPN Routers
- RV340 Dual WAN Gigabit VPN Routers
- RV340W Dual WAN Gigabit Wireless-AC VPN Routers
- RV345 Dual WAN Gigabit VPN Routers
- RV345P Dual WAN Gigabit POE VPN Routers

Solution: Upgrade to the latest version available.

PATCHES

Microsoft

Date: 08-02-2022

Description. Microsoft has released the security bulletin for the month of February, which fixes a total of 94 vulnerabilities. Of these, 51 have been rated as high severity, two as medium severity and 41 have not yet been assigned a severity level. The fixed vulnerabilities include a zero-day vulnerability, although there is no known published exploit yet. By exploiting some of the vulnerabilities, a remote attacker could take control of the compromised system.

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

Affected Products:
Some of the products affected are:

- Azure Data Explorer
- Kestrel Web Server
- Microsoft Dynamics
- Microsoft Dynamics GP
- Microsoft Edge (Chromium-based)
- Microsoft Office
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft OneDrive
- Microsoft Teams
- Microsoft Windows Codecs Library

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

Android

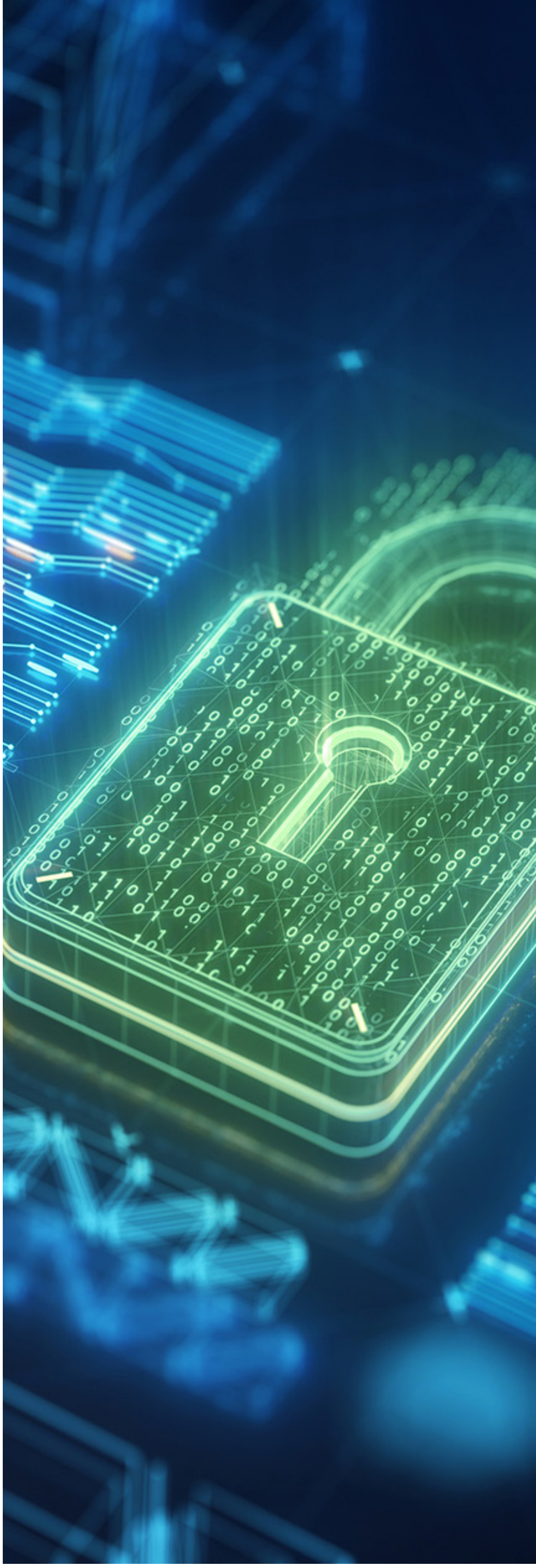
Date: 05-02-2022

Description. The January monthly Android security patch fixes 14 high severity vulnerabilities, 11 affecting the system and 3 affecting kernel components. Exploitation of these vulnerabilities could allow a remote attacker to perform system privilege escalation or information disclosure without the need for additional permissions or user interaction.

Link: https://source.android.com/security/bulletin/2022-02-01

Affected Products:
Android Open Source Project (AOSP): versions 9, 10, 11 and 12.

Solution: Install the latest available update.



EVENTS

RootedCON 2022

March 10-12, 2022 |

The computer security conference RootedCON was born with the purpose of promoting the exchange of knowledge among members of the security community. RootedCON brings together professionals with more than 10 years of experience in the ICT Security sector, as well as renowned experts, winners and/or finalists of national and international hacking, forensic analysis, and reverse engineering competitions, in addition to regular speakers at security conferences. Among its main activities are one-day training courses distributed over the three days of the CON, advanced courses lasting more than one day that specialise in a specific subject and talks on different topics related to cybersecurity.

Link: https://www.rootedcon.com/inicio/

WICYS (Women In CyberSecurity) 2022

March 17-19, 2022|

Women in CyberSecurity (WiCyS) is the leading organisation with an international scope dedicated to bringing together women in cybersecurity from academia, research, and industry to share knowledge, experiences, networking, and mentoring. What sets WiCyS apart from other conferences is that approximately 50% of the attendees are selected scholarship students from high schools and 2-4 year institutions at all levels of education; and the other 50% of attendees are professionals at various levels in their careers.

Link: https://www.wicys.org/events/wicys-2022/

ESRM (Enterprise Security & Risk Management) 2022

March 24 , 2022 |

Enterprise Security & Risk Management has a long-established reputation for bringing together the key players, thinkers and organisations involved in the effective management of security and risk in enterprises, as well as their expertise in this area. At the forefront of human and technological innovation, Whitehall Media ESRM 2022 promises to provide a platform through which to share knowledge, expand our professional networks and discover solutions to today's security challenges.

Link: https://whitehallmedia.co.uk/esrmmar2022/

RESOURCES

New OWASP MSTG 1.4.0

OWASP has released the updated version 1.4.0 of the Mobile Security Testing Guide. Most of the new features are aimed at the Mobile App Security Checklist to make it easier to understand and improve its appearance. It offers a new, more detailed multi-language design from where cybersecurity auditors will be able to track the controls performed in their audits with greater simplicity and cleanliness.

Link: https://github.com/OWASP/owasp-mstg/releases

PwnKit (CVE-2021-4034)

The Qualys research team has discovered a memory corruption vulnerability in polkit's pkexec, a SUID-root program that is installed by default on all major Linux distributions. This easily exploitable vulnerability allows any unprivileged user to gain full root privileges on a vulnerable host by exploiting this vulnerability in its default configuration.

Link: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

Windows Forensics & Tools

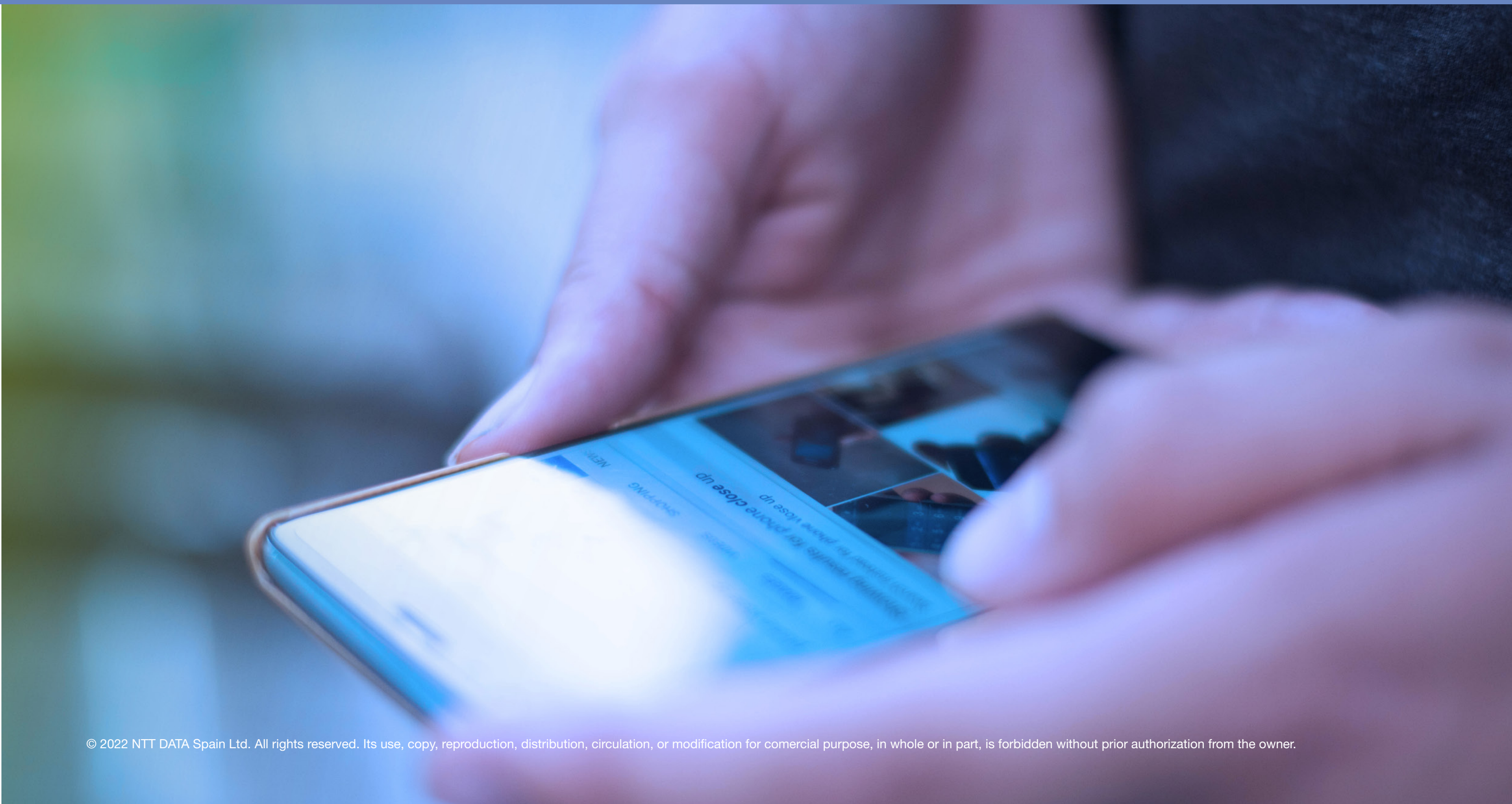
This course focuses on a set of software/tools that are used to obtain or process information in Windows. Windows Forensics contains several documented features, plus it easily allows access to the physical layers of various devices. Some of the topics covered in the course are system logs, Windows Prefetch, restoration points and relevant system files.

Enlace: https://www.cybrary.it/course/windows-forensics-and-tools/

Applications using Log4J affected by CVE-2021-44228 and its mitigation

In this Occentus corporate blog post we can find a list of products and services affected by the recently found vulnerability in the Log4j library, specifically the one related to CVE-2021-44228. This vulnerability has been classified as critical, especially due to the search capability of Log4J, combined with JNDI (Java Naming and Directory Interface).

Link: https://www.occentus.net/blog/2021/12/13/aplicaciones-log4j-cve-2021-44228/



NTT DATA
Trusted Global Innovator

powered by the
cybersecurity NTT DATA team

nttdata.com