Issue 103 | June 2025

NTT DATA

Radar

The cybersecurity magazine

Footprinting: What they know about you before you realize it

By Alexis Martín García

Before an intrusion occurs, even before an organization realizes it is being watched, a meticulous process of information gathering has already been set in motion. This process, seemingly passive and without any apparent technical trace, is the prelude to many of the most successful targeted attack campaigns. This is footprinting, a discipline in itself, which exploits everything that an organization or its employees have voluntarily exposed, or sometimes unknowingly, has involuntarily exposed to the outside, without fully understanding its operational value from the adversary's point of view.

The attacker doesn't need privileged access to start. Structured intelligence is enough for them: names, corporate emails, physical locations, network architecture, external providers, technologies used, project names or even the behavior patterns of key personnel. All this information is scattered in open sources, whether web pages, technical forums, social networks, public documents and can be collected without violating a single legal norm. It is the silent foundation upon which impersonation, intrusion, manipulation, or extortion campaigns are built.

This is where footprinting ceases to be a technical concept and becomes a strategic concern. As the dependency on digitalization grows at all levels of an organization, the surface of exposure also increases. And, therefore, the appetite of threat actors for that unmanaged exposure grows.

One of the most obvious catalysts for this risk is social engineering. When an attacker has credible, contextualized information aligned with the real processes of the organization, their chances of success increase exponentially. A generic phishing email may be ignored; but if that email references a real meeting, mentions a legitimate colleague, or replicates an internal process, the possibility of interaction from the recipient ceases to be remote.

This is not a matter of human errors, but a strategic advantage built from prior intelligence. And this is where the discipline of Cyber Threat Intelligence (CTI) comes into play. Far from being a reactive practice, focused solely on technical indicators, well-structured threat intelligence has the potential to identify patterns of external observation, infer intentions, and anticipate possible exploitation scenarios before the attacker takes action.

Footprinting, from the defender's perspective, should be understood as a dual tool: not only to identify what others could exploit, but also to establish protection priorities based on what is truly visible, accessible, and valuable from outside.

At NTT DATA our CTI teams have the capability to map the digital footprint of an organization from the adversary's point of view. This often underestimated practice allows the discovery of abandoned domains that still point to internal services, documents indexed by search engines revealing business relationships, personal profiles exposing sensitive roles, or network structures inferred through technical information inadvertently exposed in specialized forums.

And most concerning, all this information is sufficient for malicious actors to develop highly targeted attacks without the need for advanced technical tools. The attack begins in the mind of the adversary when they find the narrative that allows them to fit all the pieces together.

Therefore, discussing footprinting and social engineering should not be reserved solely for Red Team teams or internal drills. It should be part of a broader conversation about organizational resilience, information risk management, and threat modeling based on contextual intelligence.

The challenge is not to avoid being observed, something practically impossible in an interconnected world, but to control what is seen and understand the value that exposure has for those seeking to harm us. What is at stake is not only corporate privacy but the ability to withstand attacks that begin long before they are detected in a SIEM.

Alexis Martin García
Cyber Threat Intelligence & Hacking Project Manager

OpenEoX and Software End of Life Management

Cyberchronicle by Cayetano Valero and Ana Leticia Urbistondo

The efficient management of the software lifecycle is a fundamental activity to protect organizations. One of the most significant challenges in this area is the management of "End of Life" (EoL) software. When a product reaches its end of life, it stops receiving updates and vulnerability patches. Without continued support from the manufacturer, EoL software poses a latent risk to organizations (operationally and regulatory), increasing exposure to potential threats, both known and future. In this cyberchronicle, we'll explore the capabilities of this framework and how it works with EoL software.

To illustrate the impact of EoL software, Qualys published a study showing that more than 50% of the Log4j library installations vulnerable to Log4Shell were out of support when the vulnerability was published, and 98% of the Windows 7 systems affected by WannaCry were running EoL versions of Windows.

Due to the impact that EoL software can have on organizations, early and effective identification becomes a key part of the migration process to a supported alternative version before reaching End of Life.

Recently, to improve proactivity in EoL software management, the OpenEoX initiative (Open End-of-Life Exchange) has emerged, aimed at establishing a framework to unify the way information about this type of software is shared to identify it quickly and correctly, allowing for more effective action against potential threats that exploit vulnerabilities in obsolete software. Supported by companies like Cisco, IBM, or Microsoft, this framework has been developed to provide technology teams with a centralized and reliable source of information related to unsupported software, covering key points such as: known vulnerabilities, mitigation solutions, and best practices.

The OpenEoX framework offers clarity and consistency in software lifecycle management in three main aspects:

- Transparency: Making lifecycle information easily accessible and understandable.
- Efficiency: Streamlining the process for both information providers (vendors, maintainers) and consumers (users, organizations).
- Unification: Establishing a common language and data structure for lifecycle stages such as EoL, EoSSec, and EoS information.

Since OpenEoX is based on a lightweight and modular schema, it is designed to be flexible and adaptable to different environments, without the need for major changes to existing systems. Additionally, thanks to its machine-readable specification, it is possible to easily integrate OpenEoX with other standards such as CSAF/VEX (Common Security Advisory Format/Vulnerability Exploitability eXchange) or SBOMs (Software Bill of Materials). This allows both manufacturers and software maintenance managers to communicate coherently and automatically the milestones in the lifecycle of their products.

This framework provides three key benefits:

1. Early visibility of software products that will soon stop receiving security patches.
2. Lifecycle automation through scheduled alerts and coordinated actions.
3. Multisector collaboration through sharing a single data source on support statuses, shared between manufacturers and users.

To provide these benefits to organizations, as mentioned earlier, the main component of this framework focuses on standardizing milestones in the software lifecycle, proposing different specified categories that help define the lifecycle of a software product:

- General Availability (GA) – General Availability: the date when the product was officially launched to the market.
- End of Sales (EoS) – End of Sales: the last day the product is available for purchase.
- End of Security Support (EoSSec) – End of Security Support: the date when security updates/patches for the product are no longer provided.
- End of Life (EoL) – End of Life: the last date when the product stops receiving any type of support from the provider.

With OpenEoX, it is not only possible to better control the status of obsolete software products in organizations, but it also helps reduce the risk associated with these products, anticipating the need for migrations of these products and improving vulnerability management initiatives in organizations by incorporating lifecycle-based automations. Especially considering that a considerable number of threats begin with the exploitation of public vulnerabilities associated with obsolete software products.

Since the security of systems depends on effective management of technical debt, a framework that allows for proactive and homogeneous management of associated technological risks is essential, significantly improving the planning of software maintenance and the transition to new technologies.

Cayetano Valero
Cybersecurity Lead Analyst

Ana Leticia Urbistondo
Cybersecurity Analyst

Surface Test: Digital X-Ray of Corporate Exposure

Article by Carlos Barrios

In the hyperconnected era we live in, organizations are more exposed than ever. Every digital asset, every employee with a presence on social media, and every line of code published on the internet contribute to expanding a company's external attack surface. This reality demands that Digital Surveillance departments conduct a systematic and continuous exercise known as surface test, a deep x-ray of the corporate digital footprint.

Social Engineering and Digital Footprint: The Starting Point

You cannot talk about surface testing without understanding that the main objective of cybercriminals is to find vulnerabilities accessible from the outside. Social engineering remains one of the most effective weapons. According to data from Splunk, 98% of cyberattacks are based on emotional or psychological manipulation techniques to gain access to confidential information.

Why is it so effective? Because it attacks the weakest link: people. And to exploit people, attackers need prior information: roles, internal structures, technologies used, domain names, subdomains, leaked passwords... All of this is part of the digital footprint that an organization leaves exposed to the world without even realizing it.

Here are some of the most common tactics:

• Phishing: Involves sending emails or creating fake websites that mimic legitimate entities to deceive the user and obtain personal data or credentials.

• Shoulder Surfing: An observation technique where the attacker obtains sensitive information by directly watching (or using tools like binoculars) while the victim enters it on their device.

• Dumpster Diving: Involves searching through corporate trash for discarded documents that may contain useful information, such as internal manuals, printed passwords, organizational charts, or old devices.

• Role Playing (Pretexting): The attacker impersonates a trusted figure (like technical support or an executive) through calls, emails, or chats to persuade the victim and obtain sensitive information.

• Trojan Horse: Deceives the victim into downloading and installing malicious software that opens a backdoor in the system, giving the attacker remote control of the device.

• Web Crawling: Attackers gather information from corporate websites, social media, or forums to understand the organization's structure, identify key contacts, and prepare more effective targeted attacks.

• Reverse Social Engineering: The attacker simulates a problem in the system and presents themselves as the only reliable solution. They gain the victim's trust by “helping” them, thus gaining access to confidential information. This approach combines sabotage, marketing, and support to create dependency in the victim.

External Recognition: The First Step of the Attack (and Defense)

The surface testing process begins just as a malicious actor would: with passive reconnaissance. Using open-source intelligence (OSINT) techniques, CTI analysts gather public data about the organization from multiple fronts:

- Corporate websites
- Social media (especially of employees)
- WHOIS and DNS
- Public forums and deep/dark web
- Job offers and press releases

This recognition reveals that the organization often is unaware it has exposed, including:

- Forgotten or inherited servers
- Unnecessary open ports
- Unprotected subdomains
- Unauthorized applications by IT (Shadow IT)
- Leaked corporate credentials
- Social media posts with sensitive metadata

OSINT as a key tool for surface testing

Tools like Shodan or Censys allow scanning the public network to identify services and connected devices: from routers and cameras to email servers with vulnerable configurations.

No privileged access is required: all is open and available information. This is precisely what makes the surface test such a powerful and critical tool: if we can see it, an attacker can too.

The surface test as a methodology does not only seek to gather information but also analyze, classify, prioritize, and report risks. It is about building an accurate inventory of the digital assets accessible from the internet, assessing their criticality, and generating alerts for any anomalous or unauthorized exposure.

In a modern organization, the Digital Surveillance area not only monitors external threats in open sources or the dark web. It also performs proactive surface testing tasks, including:

- Discovery of unlisted digital assets
- Identification of exposed credentials
- Monitoring mentions and leaks on clandestine platforms
- Assessment of reputational and brand risks
- Alerts about possible social engineering or spear phishing campaigns

These capabilities allow acting before an incident occurs, transforming the reactive defense posture into an anticipatory defense based on intelligence.

A key maxim in cybersecurity is: “You cannot protect what you cannot see.” The surface test reveals just that: what is exposed but invisible to the organization itself and it is precisely in large companies with multiple locations, recent mergers, or decentralized structures that orphaned assets, insecure configurations, or unmonitored services may exist. A simple test environment left open by a developer can become the entry point for a larger attack.

From theory to action: managing the attack surface

The management of the external attack surface (ASM, for its acronym in English) is a continuous process, which involves:

1. Discovery: inventory all exposed assets.
2. Classification: determine the type of asset, its function, and criticality.
3. Analysis: look for vulnerabilities, weak configurations, or associated credentials.
4. Prioritization: define the real risk and potential impact.
5. Mitigation and follow-up: coordinate with IT, SOC, or development teams.

This requires not only technology but also processes, talent, and strategic vision. And above all, a clear understanding that the attack surface does not end at the firewall perimeter, but extends as far as the digital footprints of employees and systems on the internet.

Conducting a surface test is not a one-time action, but a strategic practice. It is the foundation upon which hardening policies are built, patches are prioritized, access controls are strengthened, and social engineering campaigns are anticipated.

In the current landscape, where attacks are increasingly directed at people and not just systems, understanding and anticipating adversary behavior becomes a priority. Social engineering, combined with reconnaissance techniques like footprinting and the use of open-source intelligence (OSINT), shows that attackers do not need to breach a technical infrastructure if they can exploit the weakest link: the human factor.

From the Digital Surveillance teams, it is essential not only to monitor the exposed digital infrastructure but also to adopt an offensive mindset to proactively detect attack vectors, uncontrolled digital footprints, leaked credentials, presence on the dark web, and early signs of threats. The management of the external attack surface (EASM) and continuous analysis of the digital environment are key tools to anticipate risks, minimize exposure, and protect both technological assets and critical information.

Only by understanding how attackers think and act —and using their own tools and techniques for defensive purposes— can we build truly effective protection strategies. In this new paradigm, digital surveillance ceases to be a complement and becomes an essential pillar of any modern cybersecurity program.

Carlos Barrios
Cyber Threat Intelligence Lead Analyst

Quantum technologies

Quantum Space by María Gutiérrez

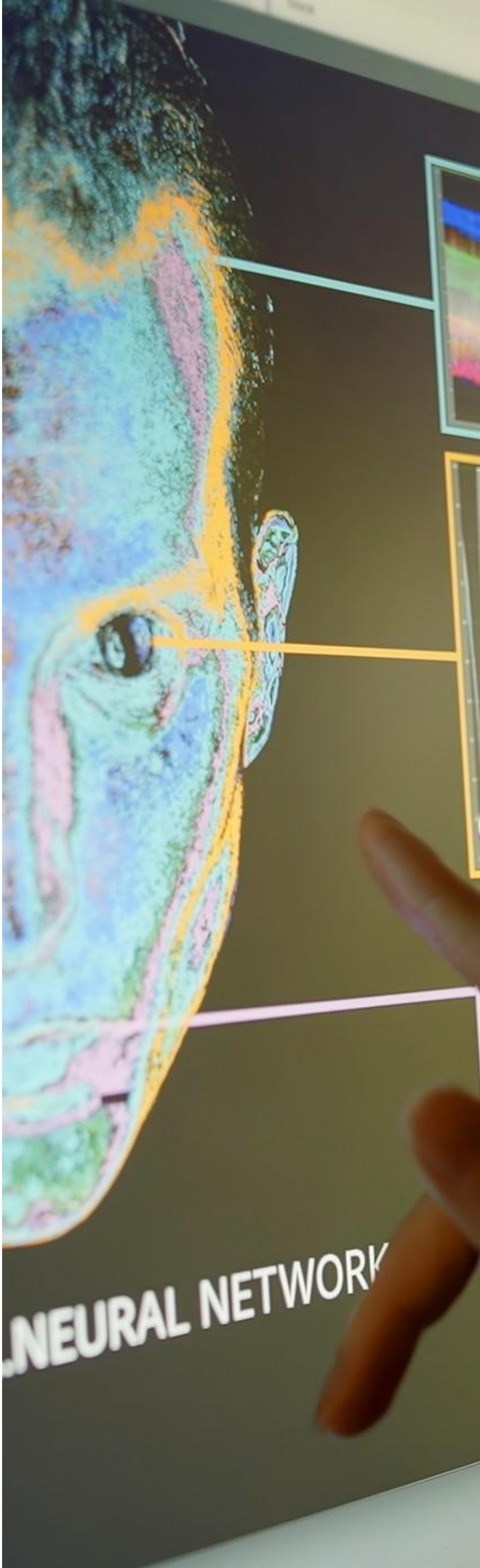
As we have already mentioned, 2025 has been proclaimed the International Year of Quantum Science and Technology by the UN. Upon hearing this, most of us think of quantum computing, but the quantum industry encompasses much more. In fact, the broader category of quantum technologies leverages the behavior of particles for a wide range of applications, including navigation tools, enhanced imaging technology, and extremely precise timing devices.

In this article, we will focus on "quantum sensing," an application of quantum technology that allows for measuring physical phenomena with unprecedented precision, sensitivity, and resolution. These sensors can exceed the limits of classical devices and offer innovative solutions to industrial and social problems.

Unlike classical sensors, quantum sensors can record tiny variations in the environment (movement, electromagnetic fields, etc.) by taking advantage of the fact that quantum states are extremely sensitive to external disturbances.

In this way, they achieve extraordinary spatial resolutions and sensitivities that open new possibilities in various fields. For instance, in the healthcare and biomedical sector, quantum sensing promises to revolutionize imaging diagnostic techniques and physiological process monitoring. Optical pumping magnetometers (OPM), which are quantum sensors based on gaseous atoms, allow for magnetoencephalography (MEG) to be performed more flexibly than conventional systems.

Portable helmets filled with these OPM sensors already exist; they record the magnetic fields produced by brain activity, allowing the patient to move freely during the clinical examination.



This opens the door to studies of the brain in more natural conditions and new diagnostic applications.

In the defense sector, quantum sensors offer strategic advantages in detection and navigation. An area of great interest is quantum inertial navigation, which would allow military vehicles (submarines, ships, or aircraft) to orient themselves with high precision without relying on GPS.

Currently, if a submarine operates submerged for weeks, its conventional inertial system accumulates error (drift) and eventually must surface to recalibrate with GPS.

With quantum accelerometers and gyroscopes based on cold atoms, this drift could be eliminated, providing continuous and secure navigation even in environments where satellite signals are blocked or vulnerable to interference.

Outer space, for its part, is an ideal environment to take advantage of quantum sensing, for example, in planetary exploration and astronomy. Under microgravity conditions, atomic interferometers can achieve longer measurement times and, therefore, greater sensitivity than on Earth. This also allows for the development of spatial quantum gravimeters that measure the Earth's gravitational field or other celestial bodies with high resolution.

For example, future missions could map the mass distribution of a planet or moon by detecting subtle gravitational variations, as different materials (water, rock, ice) cause slight local differences in gravity.

In summary, quantum sensing is emerging as a disruptive technology that brings the strange phenomena of quantum physics from the laboratory to real-world applications, underscoring that quantum technology is not just about computation.

The Digital Footprint in Focus - Analysis, Risks, and Protection in 2025

Trends by Joel Perez and Rodrigo Rey

In the digital age, we all leave a trace on the Internet: comments, photos, social profiles, public records, and more. This trace is known as digital footprint, and its analysis has become a key practice for both cybersecurity and attacks. The discipline of open-source intelligence (OSINT) is responsible for collecting and examining publicly available information on the web to turn it into useful intelligence. This information comes from various sources: social networks, forums, blogs, government records, or news, among others. Understanding one's own digital footprint or that of an organization is vital: it can reveal reputation, relationships, and potential vulnerabilities.

Modern Tools for Tracking the Digital Footprint

In recent years, numerous OSINT tools have emerged to facilitate the tracking and analysis of the digital footprint of individuals and companies. For example, platforms like Maltego or SpiderFoot allow gathering scattered data and visualizing connections between individuals, organizations, and digital assets. Other tools like Shodan act as specialized search engines for devices connected to the Internet.

Shodan allows discovering servers, cameras, or routers publicly exposed, even identifying those with weak passwords or outdated software. There are also search engines focused on social networks (social searchers) that monitor public mentions in real-time, useful for monitoring online reputation.

These automated tools save analysts time by collecting information from multiple sources, painting a detailed map of an individual's online presence.

Vulnerabilities Exposed Through Public Information

The digital footprint matters not only for what it says about us but also for what it can reveal in terms of security. Much seemingly innocuous information can be exploited by attackers.

A common case is the use of advanced searches like Google Dorks to locate sensitive data mistakenly indexed, such as confidential documents on public servers or lists of exposed passwords.

Similarly, OSINT tools like Shodan can uncover vulnerable systems accessible from the Internet – for example, a security camera without robust credentials or a corporate server with improperly open ports.

Another popular utility is FOCA, a tool developed in Spain that extracts metadata from public documents (PDF, Office, images) to uncover hidden information: usernames, internal file paths, software versions, and even possible internal IP addresses. All this information collected without directly entering any system allows professionals (and also criminals) to detect weak points. In security audits, OSINT helps identify leaked credentials, misconfigurations, or exposed personal data that could facilitate an attack. With enough ingenuity, public data becomes pieces of a puzzle that reveals security gaps.

Social Engineering Enhanced by the Digital Footprint

Social engineering is the art of manipulating people to gain access or confidential information, and it has been profoundly reinforced by the abundance of online data. Attackers employ OSINT techniques to gather all available data about their victims and thus personalize their deceptions.

What's the result? More credible and targeted attacks. A clear example is spear phishing or targeted phishing: instead of sending generic emails, the criminal researches their target on social networks and other sources, finding out their name, position, coworkers, likes, or habits.

With that information, they draft a very convincing email, perhaps pretending to come from a colleague or a service the victim uses, mentioning specific details to gain their trust.

In fact, nowadays, every sophisticated phishing attempt leverages detailed data to make the message seem legitimate and unique.

If the victim often posts about their travels, the hook might be a false flight confirmation; if they are an executive, they might receive an email seemingly from HR with internal information. This personalization makes it extremely difficult to distinguish the deception.

The situation has become more complex with the emergence of artificial intelligence (AI) in these tactics. Generative AI tools can produce messages in the exact style and tone that a company or person would use, automating the creation of fraudulent emails on a large scale.

There have even been reports of scams where the voice of an executive was cloned using deepfake audio, to order million-dollar transfers over the phone with a voice that sounded authentic. In summary, a person's digital footprint (their public data) is used as ammunition for highly convincing social engineering attacks.

Emerging Protection Technologies

In the face of these risks, innovative tools and practices have also emerged to protect digital identity and mitigate OSINT-based threats.

On one hand, experts recommend strengthening the fundamentals: limiting the personal information we share publicly, properly configuring privacy on social networks, and maintaining secure passwords (ideally supported by multi-factor authentication). Measures like two-step authentication (2FA/MFA) add an extra layer that has proven to significantly reduce the effectiveness of attacks based solely on stolen credentials.

On the other hand, there are specialized platforms for monitoring the digital footprint. For example, commercial identity protection services offer continuous tracking of the Internet and the dark web for personal data of the client (document numbers, emails, leaked passwords).

One case is Bitdefender Digital Identity Protection, which analyzes every corner of the web for compromised accounts, exposed passwords, or other sensitive information, alerting the user as soon as it detects a breach. Similarly, free tools like Have I Been Pwned allow anyone to check if their email or phone number has appeared in known data breaches.

Companies, for their part, can turn to solutions like ZeroFOX, which monitor social networks and other open sources to detect identity theft attempts or information leaks in real-time. Algorithms capable of analyzing videos and audios to identify deepfakes and other digital forgeries are even being developed, in order to stop sophisticated fraud before it occurs.

Finally, awareness and training remain one of the most effective defenses. Cybersecurity training programs teach employees and users to recognize phishing signals and social engineering techniques.

Through controlled attack simulations, educational platforms (for example, KnowBe4 in the corporate realm) reinforce good security habits in individuals. With a combination of cutting-edge technology and education, it is possible to significantly reduce the risk posed by the exploitation of our digital footprint.

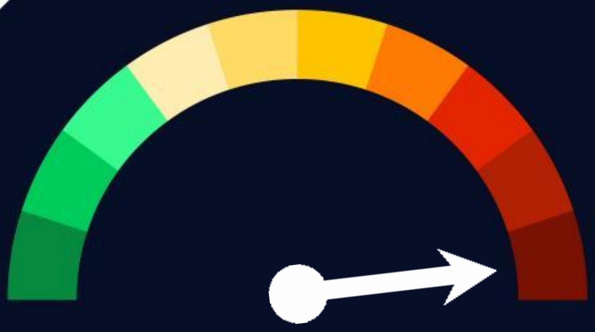
Joel Perez
Lead Architect

Rodrigo Rey
Lead Architect

Vulnerabilities

Critical vulnerability in AWS Amplify Studio

Date: May 05, 2025
CVE: CVE-2025-4318



CVSS: 9.5

CRITICAL

Description

Amazon has detected this critical vulnerability (CVE-2025-4318) affecting AWS Amplify Studio, a visual interface for developing web and mobile applications.

This vulnerability causes an input validation issue in the properties of the user interface component of AWS Amplify Studio, specifically in the package "aws-amplify/amplify-codegen-ui".

This could allow an authenticated user with permissions to create or modify components to execute arbitrary JavaScript code during the rendering and compilation process of components.

Solution

To correct this vulnerability, it is recommended to update to version 2.20.3 of AWS Amplify Studio.

Additionally, it is important to ensure that the version is updated for any related code, thereby incorporating the new changes.

Affected products

This vulnerability affects version 2.20.2 of the package "aws-amplify/amplify-codegen-ui" of AWS Amplify Studio and its previous versions.

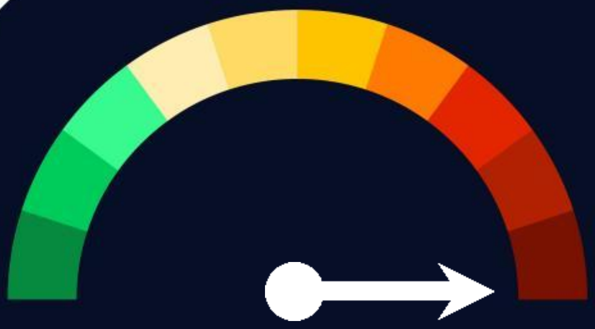
References

- incibe.es
- aws.amazon.com

Vulnerabilidades

Critical severity vulnerability in Cisco IOS XE

Date: May 07, 2025
CVE: CVE-2024-20188



CVSS: 10.0

CRITICAL

Description

Cisco has published a critical vulnerability present in its IOS XE wireless controller. This vulnerability only affects systems that have the out-of-band AP image download function enabled.

The company has indicated in its statement that this vulnerability is due to the presence of an openly exposed JSON web token in the code of the affected systems.

Through its exploitation, an unauthenticated remote attacker could upload files to the affected system, change directories, and execute commands with root privileges

Solution

It is recommended to update the products to the latest version released by the manufacturer. Furthermore, to determine if a device may be affected by this vulnerability, Cisco recommends executing the following command:

```
> show running config | include ap upgrade
```

If this command returns 'ap upgrade method https', the system would be affected by the vulnerability

Affected Products

Some of the affected products are:

- Catalyst 9800-CL wireless controllers for the cloud.
- Integrated Catalyst 9800 wireless controller for switches in the Catalyst 9300, 9400, and 9500 series

References

- incibe.es
- sec.cloudapps.cisco.com

Security patch to correct critical vulnerability in SAP NetWeaver

Date: May 09, 2025
CVE: CVE-2025-31324

Critical

Description

A critical vulnerability has been discovered in SAP NetWeaver Visual Composer (CVE-2025-20188), in the Metadata Uploader component, with a CVSS score of 10.0.

This component lacks adequate protection, allowing a remote attacker without authentication to upload arbitrary files with executable code.

The vulnerability has already been exploited, enabling the installation of web shells and other tools, and has been attributed to actors linked to groups of Chinese origin, highlighting the immediate need to apply countermeasures to mitigate the risk.

Affected products

This vulnerability affects SAP NetWeaver Visual Composer in its version 7.50, specifically the Metadata Uploader component.

The compromised systems are used by organizations in various sectors, such as energy, pharmaceuticals, or manufacturing.

Solution

It is recommended to apply the emergency update released by SAP that fixes the vulnerability, as well as to deactivate the Visual Composer component unless it is strictly necessary.

References

- thehackernews.com
- incibe.es

TLP:WHITE

Microsoft April 2025 Security Updates

Date: April 05, 2025
CVE: CVE-2025-27363 and 45 more.

High

Description

Google has released its monthly security patch for May, addressing a total of 46 vulnerabilities, including one of high severity (CVE-2025-27363) that is under active exploitation.

This vulnerability is found in the open-source font rendering library FreeType and is due to an out-of-bounds write error. This could result in remote code execution when parsing TrueType GX and variable font files.

Additionally, the patch fixes other vulnerabilities that could facilitate privilege escalation attacks, denial of service, and disclosure of confidential information.

Solution

The vulnerability affects the following Android components:

- Android Open Source Project (AOSP): versions 13, 14, and 15.
- Components from Arm, MediaTek, Imagination Technologies, and Qualcomm.

Affected products

Google recommends updating your devices to the latest available software version to address the vulnerabilities.

References

- thehackernews.com
- source.android.com

Events

Infosecurity Europe

3 June – 5 June

Infosecurity Europe, which will be held this year in London, is the leading event in the field of cybersecurity where industry professionals will gather to discuss and explore current and future challenges of security in the digital world. Among the highlighted conferences is "AI Attacks LIVE", where AI-driven cyberattacks and their mitigation will be addressed. Additionally, the event will explore the implementation of effective risk management strategies, cloud security, and the latest trends in protecting critical infrastructures.

Link

JNIC

4 – 6 June

The X National Cybersecurity Research Conference (JNIC), in collaboration with INCIBE, will be held at the University of Zaragoza. This scientific congress brings together the academic, professional, and business community to discuss advances and innovative approaches in cybersecurity. Additionally, the RENIC Research Awards in Cybersecurity will be presented for outstanding works. The event will focus on research, transfer, and training in cybersecurity.

Link

EuskalHack Security Congress VIII

20 – 21 June

The eighth edition of the EuskalHack Security Congress, which will be held in Donostia, stands out as a reference forum in cybersecurity in the Basque Country. This congress focuses on dissemination and the exchange of experiences among industry experts, covering cutting-edge topics such as the use of artificial intelligence in cybersecurity, web application security, malware analysis, and digital surveillance strategies. Attendees will have the opportunity to participate in conferences led by industry professionals and access practical workshops that strengthen collaboration and learning in new protection techniques and responses to cyberattacks.

Link

Resources

➢ CAIDO

It is a tool aimed at facilitating web analysis in security audits. It seeks to provide a modern and efficient alternative to other more traditional tools like Burp Suite.

Link

➢ YES3 Scanner

YES3 Scanner is an open-source tool that scans and analyzes the different configuration elements of AWS S3 containers to detect security risks and thus reduce them, such as public access, encryption types, ransomware protection, or the data recovery plan among many others.

Link

➢ Sniffnet

Sniffnet is an open-source tool designed for real-time network traffic monitoring and analysis. Its main goal is to capture, visualize, and analyze network traffic in a simple and accessible way compared to other more famous tools like Wireshark

Link

Subscribe to RADAR

Powered by the
cybersecurity
NTT DATA team

es.nttdata.com