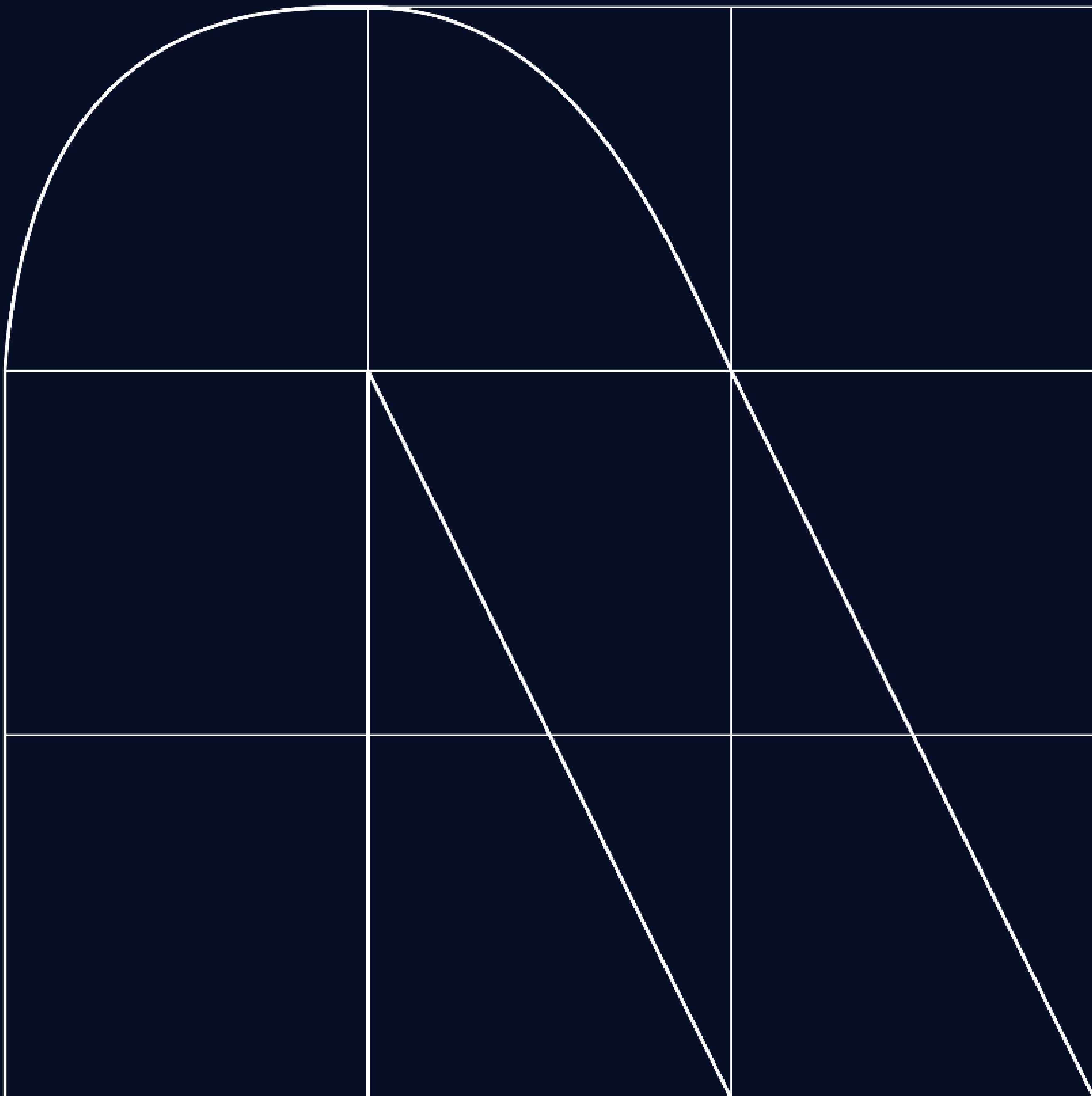
Issue 87 | February 2024

Radar

The cybersecurity magazine



The importance of knowing who the enemy is (who is behind it)

EDITORIAL by Jose Manuel Moreno

Every year, companies and organisations face an increasing number of attacks, raising the level of sophistication and causing greater economic, operational, and reputational damages. Those individuals or groups carrying out such attacks generally have clear objectives in executing them, as well as specific targets or groups of victims (sectors or industries) on which to focus.

The Cyber Threats and Trends 2023 report published by CCN-CERT in the past November highlighted the increase in the sophistication of threat actors and groups, the use of new malware families, and the evolution of artifacts used for these attacks.

Ransomware attacks continue to be the most prevalent, primarily due to the economic return that threat groups obtain from them. According to the "Cost of a Data Breach" report by IBM, the average economic damage from such attacks in the last year increased by 144% compared to 2022. The threat groups that executed the most attacks of this kind were LockBit 3.0, BlackCat (ALPHV), Hive, Conti, and REvil.

When facing the challenge of protecting our organisations, it is crucial to know who the enemy is, who is behind these attacks. The fact is that not all threat groups have the same objectives or use the same techniques and tactics, and this is where Threat Intelligence becomes particularly relevant.

What does Threat Intelligence offer, and how can we gain an advantage over the adversary?

The goal of Threat Intelligence services is for an organisation to obtain as much information as possible about the state of cybersecurity, identify threat groups that may attack our organisation, understand the tactics, techniques, and procedures (TTP) used by these actors, and, as far as possible, iteratively track the attacks carried out by these groups on any organisation worldwide.

But once all this information is obtained, what do we do with it? Data alone does not improve or enhance the resilience of our organisation. That is why there are other preventive services that take Threat Intelligence as a starting point..

- **Threat Hunting** is a proactive preventive service that aims to actively analyse the records of an organisation's main defense lines, searching for any signs of suspicious activity. It leverages intelligence information, identifying key actors and the traces they leave on victims, to trace those patterns in our security logs (primarily in the SIEM). This proactive service can thus identify the presence of these threat groups in our systems early on and activate specific protection levels to guard against them.

- **Detection Rules** is another preventive service that allows enhancing the resilience of our organisation by creating or implementing additional detection rules to identify the presence or attempted presence of threat groups against our organisation. The Threat Intelligence team should provide as much information as possible about the malware, exploits, or vulnerabilities used by our adversaries, enabling this service to create accurate detection systems.

- **Adversary Simulation** is a service that aims to simulate the behaviour of these threat groups against our organisation. It is essentially a Red Team exercise designed to mimic the actions of a threat group against our own organisation. The objective of this team is to use, as much as possible, the same Tactics, Techniques, and Procedures (TTP) as the threat groups and employ the tools and exploits most commonly used by the "imitated" groups. This service holds significant value in protecting our organisation and assessing its resilience against these actors.

As we can see, the evolution and level of sophistication of our adversaries compel us to understand them in as much detail as possible and use that information to increase the resilience of our organisation.

José Manuel Moreno
Cybersecurity Director

Experts Warn of the Imminent Danger of AI in Phishing

Cyberchronicles by Adrián Álvarez Sánchez y Pablo García Díaz

Hence, companies like Trend Micro consistently warn about the dangers of large language models. This is because these models can not only conduct massive scams simultaneously but also generate empathy and trust among potential victims. The ability to automate and personalise attacks makes them even more dangerous and challenging to detect.

Orange suffers a cyberattack; the specific password breached was "ripeadmin," and it was so simple that anyone could have guessed it. The attacker gained access to the account as an administrator and made changes to the global routing table, causing Orange's customers to lose internet connectivity.

Sancho Lerena, CEO of the IT and security management company Pandora FMS, believes that "the level of cybersecurity in Spain is still below the required standard," as demonstrated by cyberattacks such as the one on Orange and the one suffered by Vodafone last year.

As expected, the attack had a significant impact on Orange users, with many experiencing connectivity issues, including difficulties accessing websites, applications, and voice and data services.

On the other hand, the telecommunications company Tigo reported a cybersecurity incident affecting the normal supply of specific services to a limited group of corporate segment customers, not affecting any other mass or corporate telephony, internet, or electronic wallet services.

In a separate incident, a cyberattack successfully breached the computer systems of *Carrefour Servicios Financieros* (Carrefour Financial Services), extracting personal information from their customers. According to the company, the stolen information includes "basic personal data, contact information, ID numbers, among other details."

Information like that stolen from Carrefour's financial service is considered highly sensitive for personal cybersecurity.

Possessing such information doesn't enable an attacker to directly withdraw money from the victim's bank account or make unauthorised purchases on their behalf. However, it greatly facilitates identity theft and scams. Currently, there are several active attack campaigns of this kind in Spain.

Certain versions of org.apache.struts:struts2-core have been found to be vulnerable to remote code execution (RCE) through file upload parameter manipulation, allowing for "path traversal" (CVE-2023-50164). Under specific conditions, it is possible to upload a malicious file that can be executed on the server. Instances like this underscore the importance of testing and sanitising all server inputs before incorporating them into production applications.

Discord-Recon is a bot designed for bug bounty reconnaissance, automated scanning, and information gathering through a Discord server. An attacker could execute Shell commands on the server without having an administrator role. Developers have taken action and successfully mitigated this vulnerability in version 0.0.8 of the bot. This highlights the importance of not using tools or programs from unsecure sources that have not undergone certain security tests on public servers (CVE-2024-21663).

Moreover, new CVEs have been identified, such as CVE-2023-51448, addressing a vulnerability within the SNMP notification receivers function of Cacti-s. This could allow a threat actor to disclose all contents of the Cacti database or, depending on the database configuration, even enable remote code execution (RCE).

OT Cybersecurity: How to Manage an Industrial Audit

By Alejandro Alonso Rodríguez

In today's digital era, cybersecurity has become a fundamental pillar for all industries. However, in the industrial domain, its importance is even greater. Industrial cybersecurity is concerned with safeguarding Industrial Control Systems (ICS), which are critical for the operation of our critical infrastructures. These systems, encompassing a variety of devices and networks, are responsible for monitoring and controlling industrial processes in sectors such as energy, manufacturing, transportation, and utilities.

As these sectors become increasingly digitised and interconnected, they also become more vulnerable to a variety of cyber threats. From state-sponsored attacks to incidents caused by human errors, threats to industrial cybersecurity are diverse and constantly evolving. This article will delve into the significance of industrial cybersecurity, current threats, and how organisations can effectively protect themselves in this ever-changing digital landscape.

In the latest report from Claroty, titled "The Global State of Industrial Cybersecurity 2023: New Technologies, Persistent Threats and Maturing Defenses" (https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity-2023), it is concluded that 75% of industrial companies have been targeted by ransomware. Out of the total organisations affected by ransomware, approximately 69% had to pay the ransom. This highlights several facts:

- Despite 47% of surveyed companies expressing concern about security, the Operational Technology (OT) realm is far from the security maturity seen in the Information Technology (IT) domain. Given the 20-year lifecycle of industrial systems, legacy systems or insecure protocols are often encountered, originally not prepared for integration with the IT world, let alone new threats.

- Despite new industrial cybersecurity standards and efforts towards a common regulatory framework for OT process integrity, many companies still lack clear governance to prepare them against cyber incidents in production environments.

One of the objectives of the NTT DATA OT cybersecurity division is precisely to establish a roadmap for industrial sector companies to achieve an optimal level of maturity in dealing with these threats. To achieve this, one of the primary tools is regulatory frameworks, with two prominent ones being NIST 800-82 and ISA 62443.

The NIST 800-82 and ISA 62443 standards are crucial reference frameworks in the field of cybersecurity, specifically designed to ensure the security of Industrial Control Systems (ICS) and automation systems. Both regulations address the critical need to protect critical infrastructures and industrial processes against cyber threats, which could have devastating consequences.

The NIST 800-82, developed by the United States National Institute of Standards and Technology (NIST), focuses on providing guidelines and recommendations for the security of industrial control systems. This document covers everything from risk assessment to the implementation of effective security measures, ensuring the integrity, confidentiality, and availability of systems in industrial environments.

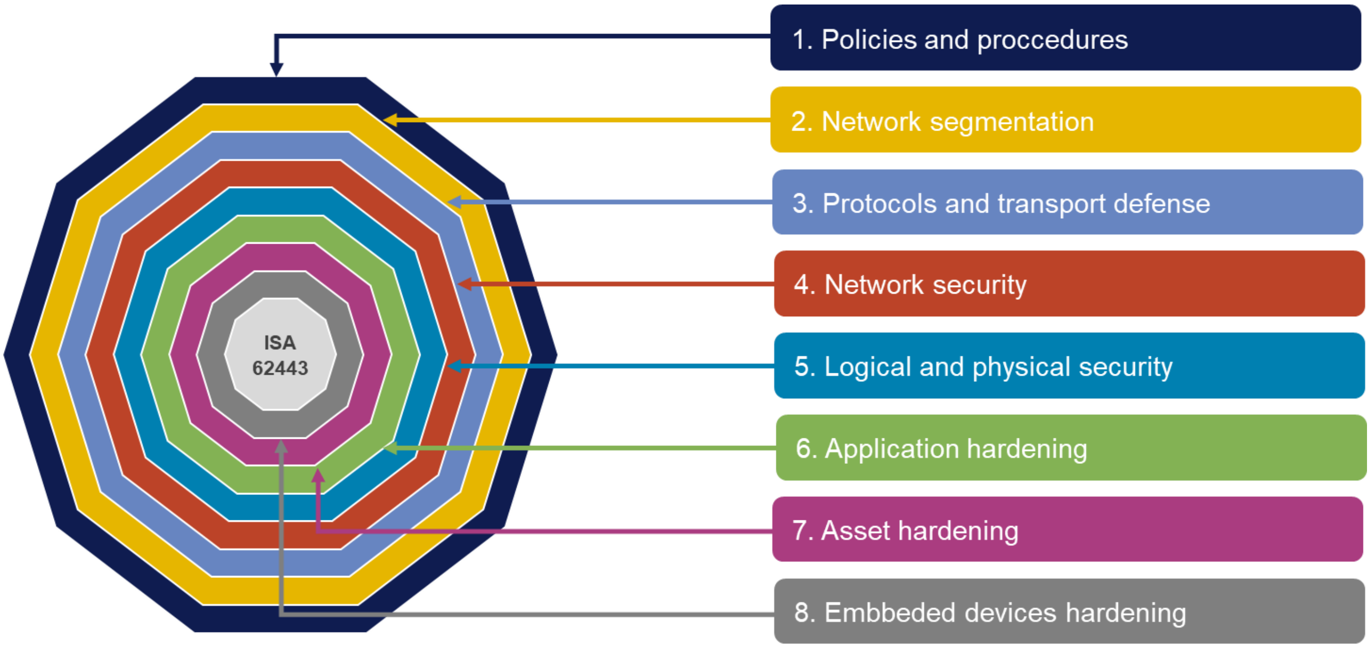
On the other hand, the ISA 62443 standard, created by the International Society of Automation (ISA), is a global standard focusing on the cybersecurity of automation and control systems. This framework provides a comprehensive structure for the identification, assessment, and mitigation of cybersecurity risks in control systems, considering specific aspects of security in industrial processes.

Both regulations are essential for establishing robust cybersecurity practices in industrial environments, contributing to the protection of critical assets, operational continuity, and safeguarding the integrity of industrial processes against growing threats.

However, it is crucial to avoid "paper consultancy" and not limit cybersecurity to a checklist of controls. It is necessary to add value, ensuring that both the strategic and technical aspects progress hand in hand during an OT cybersecurity project. That's why, at NTT DATA, during an OT governance project, we follow several stages, each of which is deeper, more technical, and more detailed than the previous one.

There are eight fundamental levels that must be reviewed and followed when undertaking an industrial cybersecurity project:

1. Policies, Procedures, and Awareness: The foundation of cybersecurity in operational environments lies in establishing robust policies and procedures. These guidelines provide the necessary framework to address threats in industrial control systems. Employee awareness, on the other hand, is equally essential, fostering a deep understanding of risks and promoting secure practices. Well-informed staff serves as a crucial line of defense against potential attacks, and the clarity of policies ensures effective implementation.


ISA
62443
1. Policies and proccedures
2. Network segmentation
3. Protocols and transport defense
4. Network security
5. Logical and physical security
6. Application hardening
7. Asset hardening
8. Embbeded devices hardening

There should be, at a minimum, a comprehensive security policy covering the OT environment and clear operational procedures (update management, permission management, backup management, etc.).

In many instances, operational knowledge is concentrated in a few individuals, leading to highly dependent processes, lack of clearly defined responsibilities, and ineffective or nonexistent internal knowledge transfer.

2. Network Segmentation: Network segmentation plays a vital role in protecting critical systems. By dividing the infrastructure into segments, the spread of threats is limited, ensuring that crucial systems operate in a controlled environment. This strategic approach minimizes risks and safeguards operational continuity, ensuring that even in the event of an intrusion, the impact remains under control.
Thanks to ISA 62443, we have the tools to define security zones, communication conduits, and tailor security measures to the requirements of each zone. Not all network zones in an OT environment require the same level of protection or attention.

3, **Defense of Protocols and Transport:** Security at the transport and protocol layers is essential to maintain the integrity of communications in industrial environments. Resisting attacks on these layers means ensuring the authenticity and confidentiality of transmitted data. Implementing robust security measures in this area is crucial to protect communication between devices and control systems.
Many OT protocols used today are inherently insecure (Modbus, Profinet-DCP, etc.). However, this does not mean that we cannot implement perimeter security measures or mitigating measures to contain attacks in case one of their vulnerabilities is exploited.

4, Network Security: The effective configuration and management of network devices are the cornerstones of a secure network. Firewalls, intrusion prevention systems, and real-time detection and response are key elements in defending against cyber threats. A well-protected network provides the necessary foundation for the secure and reliable operation of industrial control systems.
One key aspect when dealing with operational environments is visibility. We cannot protect what we cannot see. Therefore, the deployment of asset monitoring and surveillance systems is important.

Many current systems such as Nozomi, Claroty, Armis, etc., are perfectly adapted to passively discover assets. Controlling our OT assets makes us aware of our attack surface and allows us to prioritise vulnerability resolution, segmentation, and attack containment.

Equally important is the analysis of network policies implemented in elements such as firewalls. Often, temporary or weak policies are established with the trust that they will be brief and well-controlled. However, it is precisely poorly fortified or improperly implemented network security elements that serve as entry points for attackers. A poorly implemented firewall is worse than not installing a firewall.

5, Physical and Logical Security: Physical security is the first line of defense against unauthorised access, while access controls and surveillance add layers of protection. Logical security, through identity and access management, complements these measures, ensuring that only authorised personnel have access to critical systems and data. The combination of physical and logical approaches creates a robust barrier against internal and external threats.

6, Application Hardening: Application security is essential for preventing vulnerabilities. Application hardening involves proper configuration and proactive patch management. This measure aims to prevent the exploitation of potential vulnerabilities, ensuring that applications used in control systems are resilient and secure. Additionally, it is vital to have control systems for applications that may or may not be installed on our engineering stations or OT area computers.

Fortunately, many manufacturers have developed software whitelisting and blacklisting solutions tailored to these systems. With these solutions, we can even integrate alerts into our SIEM to act quickly against malicious or unauthorised programs in our network.

Similarly, many of these solutions help us monitor and protect our systems against one of the most common malware entry vectors in OT: USB devices.

7, Asset Hardening: Secure configuration of assets such as servers, workstations, PLCs, SCADA systems, etc., is crucial for protection against threats. Effective management of accounts and passwords, along with access controls, strengthens the security of these assets. These measures ensure that critical systems and data are protected against unauthorised access and unwanted manipulations. It is important to have best practice guides after the installation of new equipment. Often, default values and services implemented directly by the manufacturer leave doors open to external attackers.

8, Embedded Device Hardening: Embedded devices, such as PLCs and SCADA systems, require specific measures to prevent unauthorised manipulations. Hardening these devices involves applying firmware updates, security patches, and protection against unauthorised manipulations. These actions are crucial to maintaining the integrity and security of processes in industrial environments. Similarly, it is important to control the software and programming of these devices. Having a system that alerts us in case the integrity of these devices is compromised or altered is crucial.

Providing this 360-degree view, both strategically and technically, adds more value to expert consultancy in OT and helps see results from the first minute of the project. In environments like OT, where availability is crucial, achieving our goal is precisely the objective.

The advent of connected and intelligent devices in the industrial world has required us to adapt not only technologies but also consultancy and the way we understand security in an area with extensive obsolescence, and where changes are not trivial.

Alejandro Alonso Rodríguez
OT Cybersecurity Manager

Disinformation in an election year

TRENDS by Miguel Tuimil

Electoral disinformation is a growing global concern involving the intentional spread of false or misleading information to influence public opinion and affect electoral outcomes. This phenomenon has intensified with the rise of social media platforms and instant messaging services, where fake news and conspiracy theories can spread rapidly. Malicious actors often exploit existing emotions and polarisations to sow discord and manipulate voters' perceptions, posing a significant threat to democracy and citizens' trust in institutions.

In 2024, electoral processes in the United States, India, Taiwan, and 40 other nations will be fertile ground for social engineering and disinformation campaigns.

According to UNESCO, electoral disinformation can be grouped into four general types:

1. **Fraud Accusations:** These are often the most widespread during elections. They aim to demonstrate organised fraud coordinated by national, local, and/or electoral authorities. Examples include photos of alleged ballot boxes with broken seals or screenshots of tally sheets with errors meant to confirm fraud. Typically, unintentional irregularities do not systematically benefit any party, while intentional ones often skew results in favor of a particular group.

2. **Claims of Ineligible Voters:** During elections, content circulates attacking minorities, claiming that migrants will vote in countries where it is not allowed or without meeting legal conditions, even when foreigner voting is permitted. There is also misinformation asserting that deceased individuals are included in the electoral registry or that the identities of deceased persons are used for voting. However, in many cases, these are errors in the registry corrected by authorities.

3. **Misinformation about the Voting Process:** False content often circulates during elections to mislead or instill fear in citizens about the voting moment. Each country has different rules that determine when a vote should be annulled or contested (i.e., not counted as valid).

4. **False Statements or Propaganda from Candidates**: This involves the editing and manipulation of photos, as well as taking images out of context. False statements use frames or logos of a media outlet with the image of a candidate and a supposed quote. Manipulated or out-of-context videos circulate, as well as parody or falsely attributed audios of the candidates.

Combating disinformation in elections requires coordinated efforts from governments, technology platforms, and citizens. Strategies include fact-checking, promoting media literacy, transparency in online political advertising, and international collaboration to address cross-border disinformation campaigns. Strengthening society's resilience to disinformation is crucial, promoting an informed and critical citizenry that can discern between truthful and deceptive information in the electoral context.

Vulnerabilities

Multiple Vulnerabilities in Juniper Secure Analytics

Date: December 28, 2023
CVEs: CVE-2023-40787 and 17 more

CVSS: 9.8

CRITICAL

Description

Recently, eighteen vulnerabilities have been reported in Juniper Secure Analytics. Out of the eighteen vulnerabilities, two are of critical severity, seven are of high severity, another seven are of medium severity, and two are of low severity.

The critical severity vulnerabilities are as follows:

- CVE-2023-40787: Vulnerability related to SQL query execution in SpringBlade V3.6.0. In particular, it occurs when user-sent parameters are not enclosed in quotes, leading to SQL injection.

- CVE-2023-46604: Vulnerability that could allow a remote attacker with network access to a Java-based OpenWire client or broker to execute arbitrary shell commands by manipulating serialised class types in the OpenWire protocol to make the client or broker (respectively) instantiate any class in the classpath.

Affected products

The vulnerability affects the following product version:

- Juniper Secure Analytics, versions up to 7.5.0 UP7.

Solution

The manufacturer recommends keeping their products always updated to the latest version to avoid security risks associated with new vulnerabilities. In particular, it is recommended to update to Juniper Secure Analytics version 7.5.0 UP7 IF03, as this update addresses the identified vulnerabilities.

Links

- www.incibe.es
- supportportal.juniper.net

SQL Injection Vulnerability in Ivanti EPM

Date: January 4, 2024
CVEs: CVE-2023-39336

CVSS: 9.6

CRITICAL

Description

Ivanti has recently discovered a critical vulnerability in its Endpoint Manager (EPM) product.

The identified vulnerability, of the SQL injection type, allows an attacker with access to the internal network to execute arbitrary SQL queries, obtaining the results of the queries without the need for authentication. This could allow an attacker to take control of devices running the Ivanti EPM agent.

Furthermore, when the central server is configured to use SQL Express, the detected vulnerability could lead to remote code execution (RCE) on the central server.

Affected products

The vulnerability affects the following versions of the Ivanti EPM product:

- Ivanti EPM 2021.
- Ivanti EPM 2022 versions prior to Service Update 5.

Solution

The manufacturer recommends updating the Ivanti EPM product to version 2022 SU5.

Links

- www.incibe.es
- forums.ivanti.com
- www.ivanti.com

Patches

CRITICAL

New security patches for Microsoft products

Date: January 10, 2024
CVE: CVE-2024-0057 and 47 more

Description

On January 10th, Microsoft released a series of updates to address multiple security vulnerabilities in its Windows operating systems and other software. In total, 48 vulnerabilities have been reported, including 2 critical, 26 important, and 20 of medium severity.

The critical vulnerabilities are detailed below:

- CVE-2024-0057: A vulnerability affecting NET, .NET Framework, and Visual Studio, where an attacker could use an untrusted X.509 certificate through an API to insert that certificate and leverage the error it returns to inject malicious code.

- CVE-2024-20674: This vulnerability affects the Windows Kerberos security protocol, where an authenticated attacker, when performing a local network impersonation, can send a malicious Kerberos message to the victim client and impersonate the Kerberos authentication server.

The remaining vulnerabilities cover various types, including privilege escalation, security feature bypass, remote code execution, information disclosure, denial of service, and identity spoofing.

Affected products

Dichas vulnerabilidades abarcan un gran número de productos Microsoft. Dichos productos pueden consultarse en: msrc.microsoft.com

Solution

Apply the corresponding security patch to the affected products.

Links

- msrc.microsoft.com
- es-la.tenable.com

CRITICAL

Critical patches for GitLab Community and Enterprise Edition

Date: January 11, 2024
CVE: CVE-2023-7028

Description

GitLab strongly recommends patching to their latest versions for GitLab Community Edition (CE) and Enterprise Edition (EE) as they contain important security fixes.

Attackers exploiting the CVE-2023-7028 vulnerability can reset passwords for GitLab user accounts. Users with two-factor authentication (2FA) are not exempt, making them vulnerable as well.

The manufacturer has confirmed that no abuse of this vulnerability has been detected on platforms managed by GitLab.

This vulnerability affects self-managed instances of GitLab running the previously described versions.

A proof of concept (PoC) and an exploit for this vulnerability have been published.

Affected products

The different versions affected by this vulnerability are as follows:

- 16.1 prior to 16.1.5
- 16.2 prior to 16.2.8
- 16.3 prior to 16.3.6
- 16.4 prior to 16.4.4
- 16.5 prior to 16.5.6
- 16.6 prior to 16.6.4
- 16.7 prior to 16.7.2

Solution

GitLab recommends administrators of GitLab instances to enable 2FA for all accounts and update to versions 16.7.2, 16.6.4, 16.5.6 of GitLab CE and EE.

Links

- about.gitlab.com
- nvd.nist.gov

Events

SANS Offensive Operations London 2024

SANS Offensive Operations London 2024 will take place both online and in-person from February 5th to 10th. There are multiple courses offering practical knowledge on specialised topics, such as Windows forensic analysis, fundamentals of security in network, endpoint, cloud environments, and penetration testing of web applications and ethical hacking.

Link

HackCon

The national cybersecurity conference in Norway, HackCon, aims each year to review around 1200 to 1400 presentations and research within highly relevant topics. The goal is to choose the absolute best presentations for HackCon. Out of all the submissions, approximately one percent (12 each year) are selected to have the opportunity to speak at HackCon. This year's event will take place from February 12th to 14th in the city of Oslo, Norway.

Link

Zero Trust World

The Zero Trust World is an event taking place in Orlando, United States from February 26th to 28th, where attendees will gain the knowledge and skills needed to move towards a zero-trust cybersecurity posture. There will be keynote sessions in the morning, afternoon working sessions, hands-on hacking labs, and an exhibition hall with vendors showcasing solutions to explore.

Link

SecureWorld Financial Services

The SecureWorld Financial Services virtual conference is a prominent event aiming to bring together industry experts in the financial sector to provide guidance on critical financial services issues and their impact on cybersecurity. Over the course of 1 day, it offers key insights into how financial institutions can prepare for cyber attacks, technological disruption, and issues related to data privacy in the financial sector.

Link

Resources

0dAI
0dAI is an AI-driven cybersecurity-focused Software as a Service (SaaS) platform. It offers a wide range of services, including malware development, social engineering, exploit development, and SOC analysis, among various others.
Link

WebCheck
WebCheck is an open-source tool that enables a comprehensive analysis of web applications, gathering relevant information such as cookies, DNS records, server geolocation, and headers.
Link

CUPP
CUPP is a tool that allows the user to create customised dictionaries with information related to the target, such as the company name, family details, or the target's birthdate, enabling a more dynamic attack.
Link

CervantesSec
CervantesSec is a collaborative open-source platform for pentesters that enables time-saving project management. It allows the development of customised templates, vulnerability management, and the assignment of roles and permissions to team members.
Link

T-Pot
T-Pot is an all-in-one honeypot platform that provides a clear visualisation of a global map with live attacks and a variety of tools to facilitate the understanding of ongoing attacks.
Link

Powered by the
cybersecurity
NTT DATA team

es.nttdata.com