This document presents the data cataloged in the studies carried out (ad-hoc and structured literature review). The access links to the pages identified in the Ad-hoc process will be listed below, while the works cataloged in the structured review can be found in the technical report available at that same link.

OWASP Internet of Things Project - OWASP

IoT Product Criteria | NIST

Top IoT Device Vulnerabilities: How To Secure IoT Devices | Fortinet

These new vulnerabilities put millions of IoT devices at risk, so patch now | ZDNet

The real dangers of vulnerable IoT devices - Infosec Resources (infosecinstitute.com)

The Main Vulnerabilities and Security Risks within IoT Devices (linkedin.com)

The Most Important Security Problems with IoT Devices (eurofins-cybersecurity.com

The identified vulnerabilities are listed on the following pages along with their respective descriptions.

Vulnerabilities Ad-hoc	Description
Account Lockout	Allowing authentication attempts after 3 - 5 login attempts even after sequences of failed attempts.
Application vulnerabilities	Recognizing that software contains vulnerabilities in the first place is an important step in securing IoT devices. Software bugs can make it possible to trigger functionality on the device that was not intended by the developers. In some cases, this could result in the attacker running their own code on the device, making it possible to extract sensitive information or attack other parties.
Incorrect access control	The services offered by an IoT device should only be accessible by the owner and people in their immediate environment whom they trust. However, this is often insufficiently enforced by a device's security system. IoT devices can trust the local network to such a degree that no further authentication or authorization is required.
Insecure 3rd party components	Associated with the use of third-party software, libraries, devices, or services that contain security flaws or known vulnerabilities. This can occur when IoT device manufacturers utilize third-party components in their products without properly assessing the security of these components or without keeping these components updated with the latest security patches.
Insecure Data Transfer and Storage	Data that IoT devices receive or transmit over networks needs to be secured and restricted from unauthorized users. This is critical to maintaining the integrity and reliability of IoT applications and organizations' decision-making processes.
Insecure Default Settings	IoT devices, like personal devices, come with default, hard-coded configurations that allow for simple configuration. However, these default settings are highly insecure and easy for attackers to crack. Once compromised, hackers can exploit vulnerabilities in a device's firmware and launch broader attacks against businesses.
Insecure Ecosystem Interfaces	Insecure ecosystem interfaces such as application programming interfaces (APIs) and mobile and web apps allow attackers to compromise a device. Organizations need to implement authentication and authorization processes that validate users and secure their cloud and mobile interfaces. Handy identity tools help the server differentiate valid devices from malicious users.
Insecure Network Services	Unnecessary or insecure network services that run on devices, particularly those that are exposed to the internet, jeopardize the availability of confidentiality, integrity/authenticity of information, and open up the risk of unauthorized remote control of IoT devices. Unrequired open ports and services that transmit information over your networks should be inspected and consider removing or disabling as a security measure (if not required).
Insecure or Outdated Components	The IoT ecosystem can be compromised by code and software vulnerabilities and legacy systems. The use of insecure or outdated components, such as open source code or third-party software, can introduce vulnerabilities that expand an organization's attack surface.

Insecure Update Mechanisms	Devices with insecure update processes are at risk of installing malicious or unauthorized code, firmware, and software. Corrupt updates can compromise IoT devices, which can be critical for organizations in the energy, healthcare and industrial sectors. Updates need to be secure and on encrypted channels, while all software must be validated and approved.
Insufficient Physical Security	If attackers have physical access to a device, they can open the device and attack the hardware. For example, by reading the contents of memory components directly, any protection software can be bypassed. In addition, the device may have debug contacts, accessible after opening the device, which provide an attacker with additional possibilities.
Insufficient Privacy Protection	User personal information stored on the device or ecosystem that is used insecurely, inappropriately, or without permission.
Intrusion ignorance	When a device is compromised, it often continues to function normally from the user's point of view. Any additional bandwidth or power usage usually goes undetected. Most devices do not have logging or alerting functionality to notify the user of any security issues.
Lack of Device Management	One of the most challenging tasks to minimize risk is managing all the devices and closing the perimeter. Device scanning and profiling allows security teams to gain visibility into their IoT devices across networks, thus considering their risks, behavior, activity, and so on.
Lack of encryption	When a device communicates in plain text, all information being exchanged with a client device or backend service can be obtained by a 'Man in the Middle'. Anyone who is able to get a foothold on the network path between a device and its endpoint can inspect network traffic and potentially obtain sensitive data such as login credentials. Even when data is encrypted, weaknesses can be present if encryption is not complete or configured incorrectly.
Lack of Trusted Execution Environment	Most IoT devices are effectively general-purpose computers that can run specific software. This makes it possible for attackers to install their own software that has functionality that is not part of the normal functioning of the device. By limiting the device's functionality and the software it can run, the possibilities of abusing the device are limited. To limit the software a device can run, code is typically signed with a cryptographic hash.
Lack of Two-factor Authentication	Lack of two-factor authentication mechanisms like a security token or fingerprint scanner
Manipulating the code execution	With the help of a JTAG adapter and gdb we can modify the firmware running on the device and bypass almost all software-based security controls. Side channel attacks can also modify the execution flow or can be used to leak interesting device information
Obtaining console access	By connecting to a serial interface, we will gain full console access to a device. Security measures often include custom bootloaders that prevent the attacker from entering single-user mode, but these can also be bypassed.

Outdated software	As vulnerabilities in software are discovered and resolved, it is important to distribute the updated version to protect against the vulnerability. This means that IoT devices must ship with updated software without any known vulnerabilities, and that they must have update functionality to fix any vulnerabilities that become known after device deployment.
Overly large attack surface	Every connection that can be made to a system presents a new set of opportunities for an attacker to discover and exploit vulnerabilities. The more services a device offers, the more services it can attack. IoT software systems often involve complex interactions between devices, servers, cloud services, and other components. The more complex the software, the larger the attack surface, due to the increased likelihood of introducing vulnerabilities.
TCP/IP Stacks	Vulnerabilities affecting TCP/IP stacks – communication protocols commonly used in IoT devices – relate to Domain Name System (DNS) implementations, which can lead to Denial of Service (DoS) or RCE (Remote Code Execution) by attackers .
Update Location Writable	Storage location for update files is world-writable, allowing firmware to be modified and distributed to all users
User interaction	Vendors can encourage secure deployment of their devices by making it easy to configure them securely. By paying due attention to usability, design, and documentation, users can be encouraged to configure secure configurations.
Username Enumeration	The ability to collect a set of valid usernames by interacting with the authentication mechanism through repeated login attempts or API queries. This vulnerability can be exploited through brute-force techniques or through more sophisticated methods, such as error message analysis or system behavior.
Vendor security posture	When security vulnerabilities are found, the vendor's reaction greatly determines the impact. The vendor has a role to receive information about potential vulnerabilities, develop a mitigation and update devices in the field. The vendor's security posture is often determined by whether the vendor has a process in place to properly handle security issues.
Weak Passwords	Weak or hardcoded passwords are among the most frequent methods attackers use to compromise IoT devices. Weak, reused passwords that are short or easy to guess are simple for attackers to crack, which they use to compromise devices and launch large-scale attacks.

Vulnerabilities Structured Review	Category	Description
Access Malicious Link	Peopleware	Users may click or interact with links designed to deceive or exploit them. Malicious links can be delivered through various channels, including email, social media, messaging platforms, or compromised websites.
Broken Authentication	Application	The process of confirming the identity or veracity of an object is known as authentication. With many IoT devices in smart environments lacking strong authentication mechanisms or access control, it becomes easy for attackers to impersonate a legitimate user and use credentials or any other information that grants them access to exploit and discover security vulnerabilities in web applications.
Buffer Overflow	Application	Buffer overflow occurs when a program or process attempts to write more data into a fixed-length block of memory, or buffer, than the buffer was designed to hold.
Centralized architecture	Network	Architecture design that centralizes control and decision-making at a single central point. This means that all information from IoT devices is sent to this central point, where it is processed and actions are taken. Devices connected to the IoT transmit processing requests and data information from their sensors directly back to the data center, where information processing and storage are performed by servers running specific applications via switches.
Channel Interference	Network	Susceptibility of IoT devices to electromagnetic or signal interference in their communication channels. These interferences can occur in various forms and may compromise the integrity and reliability of communications between IoT devices. Jamming attacks are availability attacks against the wireless medium or outward-facing sensors, where an interference device can be used to block the device's sensors from receiving signals.
Channel Voice	Device	Associated with security and privacy when IoT devices incorporate voice capabilities, such as voice-activated personal assistants, smart home control systems, or voice communication devices. In smart homes, this information can now be easily picked up by exploiting poorly protected IoT devices with integrated microphone systems, such as personal assistant services (e.g., Google Home, Amazon Echo), children's toys, and other voice-controlled appliances. These systems are vulnerable to attacks such as voice intrusion and voice masking.
Communication Overhead	Network	A situation in which the quantity of data packets transmitted between IoT devices and processing or storage systems exceeds the capacity of the network or servers, resulting in degraded performance, increased latency, or even system unavailability.
Configure network repeatedly	Network	A security vulnerability that arises when network configurations are frequently applied or modified, potentially leaving the network exposed to unauthorized access, incorrect configurations, or other security risks.
Data Inconsistency	Application	In IoT, attacks on the integrity of collected, processed, and stored data subject the associated management systems to errors or discrepancies, resulting in inaccurate, incomplete, or contradictory information.
Data Leak or Breach	Network	It refers to the leakage or breach of data in IoT networks through security vulnerabilities that allow unauthorized access, disclosure, or loss of confidential data transmitted or stored in IoT networks.
Default Configuration	Device	Often, default settings assigned by device manufacturers benefit the company rather than their users. Manufacturers frequently add or enable features that are not essential for the device's operation, which aids attackers in launching their attacks. These settings should be checked and changed immediately after purchasing and setting up the device. Default login settings of IoT devices can be exploited by attackers to gain unauthorized access to the device or to reset the password.
Device Spoofing	Device	Device spoofing refers to a technique in which an attacker disguises their device to appear as a legitimate or trusted device on a network or system. The goal is to deceive network administrators, security systems, or other devices into granting unauthorized access or privileges to the attacker. The attacker typically manipulates or falsifies identification information, such as MAC addresses, IP addresses, or device identifiers, to mask their device as another trusted device.
Eavesdropping	Network	Interception and monitoring of communications between IoT devices and management systems, without the knowledge or consent of legitimate users. This can occur at various points in device communication, primarily during wireless data transmissions. Since IoT devices transmit information wirelessly, it's easier to intercept the transmitted signals, even if the IoT devices are physically secured.

Electromagnetic Emanations Leaking	Device	Electromagnetic Emanation resulting from information processing within devices. Information collection is based on observing the electromagnetic fields of IoT devices. An example here would be electromagnetic emissions leaking from unfiltered power lines. There are demonstrations of the feasibility of measuring the power line activity of a house with such precision that they could identify what the occupants were watching on television.
Energy Restraints	Device	Smart devices, such as IoT sensors, in a cloud-based IoT big data environment can fail due to power issues. IoT devices are limited in their power consumption capacity, which can negatively affect their performance, functionality, or availability.
Fake/Malicious Node	Network	The attacker inserts a rogue node between two legitimate nodes in the network to control the flow of data between them. A malicious node could be connected to the IoT system to collect and exchange data from other devices.
Heterogeneous Communication	Network	This refers to the exchange of data and information between devices and systems that use different communication protocols, standards, or technologies within the network.
Heterogeneous Interaction	Device	The vulnerability based on the heterogeneity of interconnected IoT devices refers to the exploitation of security flaws arising from the diversity of IoT devices present in a connected environment. This heterogeneity encompasses differences in terms of hardware, software, communication protocols, and configurations among IoT devices.
Identifying the Product Vendor	Peopleware	Identification and exposure of information about the manufacturer or supplier of IoT devices, which can be exploited by adversaries for malicious purposes.
Insecure Access Management	Application	Access control is necessary to prevent unauthorized entities from gaining access to system resources and to ensure that authorized entities can only access resources to which they have permission. Therefore, reliable access control policies play an important role in preventing activities that lead to security breaches in IoT.
Insecure Data Transfer and Storage	Device	This refers to the improper exposure or compromise of information during transmission or storage. Data generated in the hardware when modified can cause an absolute difference in the data, which is subsequently sent to higher layers for processing. This vulnerability occurs because IoT devices, which are responsible for collecting and transferring data, are susceptible to various forms of attack. For example, injecting false data into the sensor is a form of attack on IoT systems, which can direct automated system decisions to behave in the manner desired by the attacker.
Insecure Firmware	Device	Security vulnerabilities present in the firmware of devices, which can be exploited by adversaries to compromise the integrity, confidentiality, or availability of the device or the information it handles. Firmware is the low-level software that controls the operation of IoT devices. Due to the heterogeneous nature of these devices, firmware is not updated frequently, leading to a variety of security threats.
Insecure Initialization	Device	Security vulnerabilities in the device boot process, which can be exploited by adversaries to compromise the integrity, authenticity, or confidentiality of the system during the boot-up and configuration process of the devices. This critical phase is when the device is powered on, and basic software and hardware components are initialized to prepare the device for operation.
Insecure Interface Configuration	Application	Web interfaces are commonly used to interact with IoT devices, allowing users to access and control their resources and settings through a browser. However, if these interfaces are not properly secured, they can pose a significant security risk. Inadequate security in an IoT web interface can lead to various vulnerabilities, including weak or predictable passwords, encryption issues, authentication failures, outdated software, and lack of access control.
Insecure Management of Data	Application	Lack of proper management and protection of the data collected, processed, and stored by IoT systems and devices. This may include a range of issues related to how data is handled throughout its lifecycle, from collection to storage and sharing. Depending on the security mechanisms used, personal information can be easily leaked, resulting in security breaches.
Insecure Password	Device	A security vulnerability occurs when passwords are weak, easy to guess, default, shared, or stored incorrectly. Passwords are a standard mechanism for authentication and protection in computer systems and applications. However, when chosen or managed inadequately, they can allow unauthorized access to accounts, devices, or sensitive information.
Insecure physical interface	Device	Security vulnerabilities related to physical interaction with the device, whether through physical connection ports, user interfaces, or other physical access points. These vulnerabilities can allow adversaries to gain unauthorized access to the device, manipulate its functionality, or compromise its security.

Insecure Server	Network	It refers to a server or backend infrastructure that is vulnerable to security threats and lacks proper safeguards to protect the data and devices connected to the network. In IoT networks, servers play a critical role in data processing, storage, and communication between devices and applications.
Insecure Software	Application	Software updates are a process that should never fail or be compromised in an IoT-based system. Attention should be paid to insecure update processes that risk installing malicious or unauthorized software, with corrupted updates that can compromise IoT devices. It is important to avoid using insecure or outdated components, such as open-source or third-party software. However, manually updating patches for each IoT device may not be feasible.
Insecure traffic control	Network	Security vulnerabilities that allow interception, manipulation, or compromise of data traffic between IoT devices and other elements of the network, such as gateways, servers, cloud services, or flaws in the network security firewall itself.
Insecure Update Mechanisms	Network	Failures in firmware, software, or other parts of IoT devices and network infrastructure updates. These update mechanisms are crucial for fixing security flaws, adding new features, and ensuring the proper performance of devices. IoT-connected resources have an increased demand for updates, and the frequency of messages causes latency, resulting in network vulnerabilities.
Insufficient Testing	Device	Most IoT devices are rapidly produced to meet the growing market demands and thus may not undergo adequate testing or adhere to any acceptable security standards or evaluation frameworks. These devices may not have been tested as rigorously as desktop/server operating systems.
Knowledge the System	Peopleware	For system knowledge vulnerability, we have two reference points: the attacker's perspective, as they are aware of the system's weaknesses and employ malware or appropriate intrusion techniques, and the user's perspective, considering the growing innovation of IoT technologies, where many users still need to understand how modern IoT devices are designed and function to better protect themselves.
Lack of Active Device Monitoring	Application	The absence of a robust system to continuously monitor the status, behavior, and activities of IoT devices on the network. Monitoring IoT devices can be challenging. This is because most existing monitoring tools and practices, especially those focused on the cloud, have traditionally been designed to monitor time-series metric data without a focus on modern IoT devices or their processes. The lack of active IoT device monitoring tools makes it difficult to achieve full network visibility in IoT-based smart environments.
Lack of Proper Authentication Mechanisms	Network	The absence or inadequacy of mechanisms that verify the identity and permissions of entities, such as devices, users, or services, attempting to access or interact with the network. Authentication is a fundamental security mechanism that ensures only authorized entities have access to the network and its resources.
Lack of Side Channel Protection	Device	A side-channel attack refers to attacks that result in the disclosure of useful information about transmitted data or the internal operation of the system through alternative paths. These side channels can be exploited by adversaries to obtain confidential information that can be gleaned through channels such as energy consumption patterns, electromagnetic emissions, response times, among others, even without direct access to the data transmitted over the network.
Lack of Strong Authentication	Device	An authentication protocol should be developed to confirm mutual trust between different objects, users, or systems by verifying their identities. This prevents an attacker from accessing the device without providing the correct credentials, bypassing authentication mechanisms, and gaining control over the device.
Lack of Strong Password	Network	The absence or improper use of strong and secure passwords for authentication and access control within the network. Passwords serve as a primary means of verifying the identity of users, devices, or services attempting to access the IoT network or its resources.
Lack of Technical Support	Peopleware	The absence or insufficient availability of resources, expertise, and assistance to deal with technical issues or provide guidance for IoT devices and networks. When there's a lack of technical support, users of IoT systems may encounter difficulties in configuration, troubleshooting, or maintaining their devices and networks.
Lack Secure Communication Protocols	Network	The lack or improper use of protocols that ensure confidentiality, integrity, and authenticity of data transmitted between IoT devices, services, and backend systems. If secure communication protocols are not in place, this introduces significant security risks.

Low Computing Power	Device	IoT devices often have limited resources, meaning they may have to rely on less robust operating systems and network protocols, making them easier to compromise. On the other hand, they collect sensitive information, exacerbating the risk. Limited processing capacity causes traditional security methods to suffer various setbacks and often fail to detect physical threats on the network.
Low Data Transmission Range	Device	Devices with low data transmission range are susceptible to attacks because they require proximity to other devices to exchange data. This means that an attacker can easily infiltrate the range of these devices to carry out proximity attacks.
Low-Quality Level Code	Application	Low-quality code in IoT environment applications refers to the presence of software development practices that result in poorly structured source code with potential security and reliability issues, due to the improper use of resources resulting in security flaws such as lack of input validation, improper password handling, or weak encryption, which can facilitate attacks.
Malicious code in-app	Application	Malicious code in IoT system applications refers to software programs or code snippets that have been developed with malicious intent and are designed to compromise the security, privacy, or proper functioning of IoT devices and related systems.
Malicious Code Injection	Device	The attacker injects malicious code into a compromised physical device, which can assist in launching further attacks. The attacker compromises a node by physically injecting malicious code into it, granting access to the IoT system. One objective of these injections is to install a compromised version of the software/firmware during wireless updates of the IoT device, which could give the adversary full remote control over the compromised device.
Non-repudiation	Application	In the context of information security, non-repudiation ensures that the sender of the information is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so that neither party can later deny having processed the information.
Obtaining Console Access	Device	When connecting to a serial interface, it's possible to gain full access to a device's console. The attacker can access the hardware and read/modify the device's default settings, which can affect privacy and authentication credentials with intentional modification of the system circuit configuration.
Personal and Social Circumstances	Peopleware	Security flaws arising from personal and social factors related to users, such as inappropriate behaviors, lack of awareness or training, negligence, or misuse of IoT devices.
Phishing	Peopleware	Phishing is used to deceive people into providing their personal information or downloading malicious software capable of spreading malware. A malicious entity attempts to redirect the device user to another server for marketing purposes or to try to deceive and steal personal information.
Physical Damage	Device	Physical damage to equipment can be natural, as a result of a calamity, or even resulting from a direct physical attack by someone. This can lead to null values at the destination or lost values, which can cause an imbalance in real-time data processing.
Physical properties of the power system	Network	It refers to security vulnerabilities that arise from the physical infrastructure and characteristics of the electrical power supply system used to support IoT devices and networks. Power systems are essential for providing the necessary electrical power to operate the devices and ensure their continuous functionality.
Physical Tampering	Device	It refers to the act of physically altering a device (e.g., RFID) or a communication link. It is important to mention that an adversary can tamper with the device and use it to introduce an impostor into the system, maliciously use the device, or use it outside of its intended functionality. This type of attack is launched when the attacker is much closer to the network device and is compelled to break the hardware without permission.
Sleep Deprivation	Device	Many IoT devices use batteries as power sources, so they only detect and transmit periodically and enter a sleep state in between. This attack aims to somehow prevent the devices from entering sleep mode or minimize the suspension period, thus depleting the battery much more rapidly than in normal use.
Social Engineering	Peopleware	The attacker manipulates system users to extract private information. This makes it easy for attackers to use social engineering to deceive IoT device users into providing data or sensitive information that can be used to access smart environment networks.

Spoofing Signal	Network	An attacker impersonates or falsifies a signal to deceive IoT devices, services, or networks into accepting unauthorized commands or providing sensitive information. Signal spoofing involves manipulating or mimicking the signals transmitted between devices or services to gain unauthorized access or manipulate the network.
SQL Injections	Application	This is one of the most well-known vulnerability points for servers that accept SQL queries and updates, where additional commands can be injected to steal information from the database or alter/delete records. In this type of attack, many attackers use SQL statements for write, delete operations, and read when the web application is being compromised by SQL injection.
Systems Low-cost	Device	In many IoT devices, there are security risks associated with production and implementation that prioritize cost reduction excessively, often at the expense of security. These devices may exhibit various weaknesses that make them more susceptible to cyberattacks.
Tag Cloning	Device	Malicious activity in which an attacker duplicates or replicates the unique identification tag of an IoT device to deceive or compromise the system. Tags are components used in technologies like RFID (Radio Frequency Identification) to identify and track devices or objects. Label cloning at the physical layer involves obtaining unique identification information from a legitimate tag and reproducing it on a counterfeit tag.
Unauthorized Access	Network	Access control is necessary to prevent unauthorized entities from accessing system resources and to ensure that authorized entities can only access the resources to which they have permission. Therefore, reliable access control policies play an important role in preventing activities that lead to a security breach in IoT.
Unprotected Physical Access	Device	It refers to the physical capture of an IoT device. This threat can be serious if IoT devices need to be deployed in areas without physical security protection.
Unsecured Network	Network	Keeping IoT devices on a separate private network also eliminates the possibility of an attacker infecting other devices and spreading malware on the network when the device is connected to unsecured public Wi-Fi networks.
Untrusted Device Acquisition	Peopleware	Users or organizations acquire and integrate IoT devices into their networks without ensuring the reliability or security of these devices.
Unused Ports Enable	Network	Unnecessary or unused network ports on IoT devices or network infrastructure are left enabled, potentially providing unauthorized access points for attackers. Unused ports are those that are not actively used for the intended purposes in the IoT network.
Vendor Security Posture	Peopleware	When security vulnerabilities are discovered, the vendor's response significantly determines the impact. The vendor plays a role in receiving information about potential vulnerabilities, developing mitigation measures, and updating devices in the field.
Weak Access Control	Device	Security flaw that allows unauthorized or malicious users to gain unauthorized access to resources, functionalities, or data of the IoT device. This vulnerability may result from an inadequate implementation of access control policies, weak authentication, or absence of robust authorization mechanisms.
Weak/lack Encryption in Communication	Network	It refers to a security vulnerability that arises when data transmitted between devices and the network is not adequately protected with strong encryption mechanisms.
Weak/lack In-app Encryption	Application	Weak or missing encryption in IoT systems applications refers to the lack of proper implementation of encryption algorithms or the use of encryption algorithms that are considered weak and easily broken. Encryption is an essential measure to protect the confidentiality, integrity and authenticity of data transmitted and stored in IoT systems
Weak/lack of Encrypt	Device	Weakness or lack of encryption in IoT devices refers to a vulnerability where the encryption mechanisms in place to protect data in transit or at rest within devices are insufficient or completely missing
Wifi De-authentication	Network	Wi-Fi de-authentication is by no means new, but in the context of the smart home, loss of Wi-Fi means loss of in-home Internet connectivity, which IoT platforms are increasingly dependent on to function. When an attacker maliciously de-authenticates or disconnects IoT devices from their Wi-Fi networks, it can lead to service interruptions, loss of connectivity, or unauthorized access to the devices or network. Wi-Fi de-authentication attacks exploit the communication protocol used by Wi-Fi networks to force devices to disconnect from their current network