Risk management report

Author: Abhi Bhise | Security Architect

Contents

1 Introduction

1.1 Task description

This report will analyze the risks associated with Industrial Internet of Things (IIoT) Devices, Smart Transportation and Smart Infrastructure Technologies. The objective is to identify and assess potential cyber security risks associated with these devices, with the help of relevant industry standards and frameworks. Considering this being the first cyber risk audit of the airport, this report will set the groundwork for the future assessments with suggestions on risk mitigation strategies for the continued and secure operation of these critical systems.

1.2 Scope

Scope of the assessment has been set as follows,

- **IIoT Devices to be analyzed:**

  1. Hikvision Surveillance Cameras (Model: **DS-2CD2xxx Series**).
  2. Honeywell Building Management Systems (Models: **Honeywell XL Web II** & **Honeywell EBI R500**).
  3. Thales Air Traffic Control Systems (Models: **TopSky ATC** & **Eurocat-C**).
  4. Thales IFE (In-Flight Entertainment) System (Model: **Thales TopSeries i5000**).
  5. Garrett Metal Detectors (Models: **Garrett PD 6500i** & **Garrett Multi Zone**).
  6. Axis Communications Network Cameras (Models: **Axis Q6032-E** & **Axis M3005-V**).
  7. Zebra ZXP Series 9 Card Printers (Model: **ZXP Series 9**).
  8. Thales IFE (In-Flight Entertainment) System (Model: **Thales TopSeries AVANT**).
  9. Garmin G1000 Integrated Flight Deck (Model: **Garmin G1000**).
  10. Frequentis VCS (Voice Communication System) (Model: **Frequentis VCS 3020X**).

- **Cyber Security Risks:**
  Identifying and analyzing potential cyber security threats and their potential impact on the airport's operations, including safety, security, and business continuity.

- **Risk Management Frameworks:**
  Evaluating the suitability of various risk management frameworks for addressing IIoT security challenges within the airport environment.

- **Risk Mitigation Strategies:**
  Developing and recommending appropriate risk mitigation controls and measures to address identified vulnerabilities.

1.3 Standards and Frameworks

For this specific assessment the identified potential Risk Management Standards and Frameworks are as follows –

- Standards
    - International Standards Organization (ISO) Standards - ISO 27001
    - International Electrotechnical Commission (IEC) Standards - IEC 62443

- Frameworks
    - NIST Cybersecurity Framework
    - MITRE ATT&CK Framework

- Aviation-Specific Standards and Guidance
    - Aviation Information Sharing and Analysis Center (AISAC) Guidelines
    - ICAO (International Civil Aviation Organization) Standards
    - EUROCONTROL Standards

As mentioned earlier, this being the first risk assessment of the airport, it is very important to select the best possible standard and framework to analyze the risk. The next section of report will review these options in more details.

2 Risk Management Standards and Frameworks

2.1 Suitability of Industry Security standards

There are several well documented standards that are available to analyze the risks and vulnerabilities of an airport. The most common ones are ISO 27001 and IEC 62443 published by International Standards Organization (ISO) Standards and International Electrotechnical Commission (IEC) Standards respectively.

ISO 27001

ISO 27001 is an internationally recognized standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides a framework for organizations to manage and mitigate information security risks, ensuring the confidentiality, integrity, and availability of their sensitive information.

Suitability:

- Comprehensive framework covering a wide range of information security controls.
- Internationally recognized and well-established standard.
- Helps establish a strong overall information security management system.

Cons:

- May be less specific to the unique needs of industrial control systems.
- Can be complex to implement and maintain at the initial stage.

IEC 62443

The IEC 62443 series of standards provide a framework for securing industrial automation and control systems (IACS), addressing cybersecurity concerns specific to operational technology (OT) environments.

Suitability:

- Specifically designed for industrial automation and control systems.
- Addresses the unique cybersecurity challenges of IIoT devices.
- Provides a structured approach to assessing and mitigating risks within industrial environments.

Cons:

- May not cover all aspects of information security relevant to an airport environment.
- Designed exclusively for industrial control systems, which is hard fit for an airport.

2.2 Aviation-Specific Standards and Guidance

There are three main guidelines and standard that are specifically designed for aviation industry. These are AISAC Guidelines, ICAO Standards, EUROCONTROL Standards. Although they are general guidelines and most of them are outdated with the current fast changing world.

AISAC Guidelines

The Aviation Information Sharing and Analysis Center (AISAC) Guidelines provide best practices and recommendations for cybersecurity within the aviation industry, focusing on threat intelligence sharing and incident response.

Suitability:

- Tailored to the aviation industry's specific cybersecurity threats and vulnerabilities.
- Offers valuable insights into best practices for protecting aviation systems.

Cons:

- May not provide as comprehensive a framework for implementing and managing an overall information security management system compared to standards like ISO 27001.
- Focus may be more on threat intelligence sharing and incident response than on the detailed implementation of security controls within individual systems.
- Little outdated compared to other standards.

ICAO Standards

ICAO Standards and Recommended Practices are a set of global standards and guidance developed by the International Civil Aviation Organization to ensure the safe and efficient operation of international air transport. While primarily focused on safety, they also encompass aspects of aviation security, including cybersecurity.

Suitability:

- Globally recognized and widely adopted standards.
- Provide a strong foundation for ensuring aviation safety and security.
- Offer guidance on various aspects of aviation operations, including cybersecurity.

Cons:

- May not be as specific to the operational technology (OT) aspects of IIoT devices.
- Focus may be more on high-level principles rather than detailed technical implementation guidance.

EUROCONTROL Standards

EUROCONTROL Standards provide technical and operational standards for European air traffic management, aiming to enhance safety, interoperability, and efficiency within the European airspace.

Suitability:

- Relevant for European air traffic management systems.
- Offer valuable insights into the specific challenges and best practices within the European aviation context.

Cons:

- May have limited applicability beyond the European region.
- Focus may be more on air traffic management systems specifically, rather than encompassing the broader range of IIoT devices security.

2.3 Cyber security frameworks

Apart from above mentioned standards there are some frameworks to setup and maintain cyber security controls. They provide very specific details and are most up to date with the current cyber threat landscape.

NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) is a voluntary set of guidelines designed to help organizations assess and improve their ability to prevent, detect, and respond to cybersecurity risks. It emphasizes a risk-based approach and provides a flexible framework that can be adapted to fit the specific needs and priorities of different organizations.

Suitability:

- Very comprehensive, covers a wide range of cybersecurity activities across the entire lifecycle.
- It is flexible and can be adapted to fit organizations of various sizes and complexities.
- Focuses on managing cybersecurity risk based on the specific needs and priorities of the organization.
- Widely adopted and recognized by various industries and government agencies.

Cons:

- High-level framework, requiring further interpretation and implementation guidance.

MITRE ATT&CK Framework

The MITRE ATT&CK Framework is a globally-accessible knowledge base of adversary tactics, techniques, and procedures (TTPs) that cyber-adversaries employ during cyberattacks. It helps organizations understand how attackers operate and prioritize their defenses accordingly.

Suitability:

- More threat-focused and provides a structured knowledge base of adversary tactics, techniques, and procedures (TTPs).
- Applicable across various technologies and platforms.

Cons:

- Can be complex to understand and apply effectively.
- Primarily focused on understanding and defending against threats, rather than providing a comprehensive risk management framework.
- Hard to implement in the initial stages, mostly used to test the security controls after they are deployed.

Final decision:

As we are setting the ground work for all future cyber security audits, NIST framework suits perfectly to our needs.

CSF provides a structured approach to assessing and improving cybersecurity controls across the entire organization. This structured approach is required for an initial audit where a comprehensive understanding of the airport's current security state is considered. Plus, NIST is highly adaptable and can be tailored to the specific needs and priorities of the airport. This flexibility should allow auditors to focus on the most critical areas of concern, such as the security of critical infrastructure systems, air traffic control systems, and passenger safety.

Furthermore, the NIST focuses on a risk-based approach, enabling auditors to prioritize efforts based on the potential impact of cybersecurity incidents on airport operations, safety, and security. NIST also shared the most comprehensible and detailed vulnerability database (NVD) with mitigation suggestions. This would be huge help to identify critical risks first. Mitigating these risks first should provide most effect with least amount of time. And that is exactly what we are strategizing for this first audit, “Target low hanging fruit first”. By focusing on the most significant risks, the audit can be more efficient and effective in identifying and addressing critical vulnerabilities.

2 Risks assessment

2.1 Risk Strategy

Airport authorities have taken a very good initiative to do the risk analysis. The risk analysis of all the assets on regular basis is very important in maintaining the operational continuity and avoid any losses. It is also very crucial for the safety of the passengers using the services of airport.

The airport has not been audited for last 12 years which might have exposed its various IT assets to various risks. For such cases, a step by step approach is necessary and we have to stick to realistic goals. Hence, we propose the **“Low hanging fruit” strategy**. Target the IT infra risks and vulnerability that has been well documented and should be easy to fix in less time. This will ensure the effectiveness as we expect to see considerable amount of security enhancement in comparatively less time.

Considering this strategy, well documented risks of IT assets are analyzed in the next section.

2.2 Risk analysis

For many these devices there are already well documented CVEs available which needs fixing. Each identified and documented vulnerabilities are mentioned one device at a time the table below.

Some of the devices do not have any vulnerabilities documented in National Vulnerability Database (NVD) and hence might require further analysis. It is recommended to conduct a separate pen testing of these devices to analyze the likelihood, impact and severity of these devices. Currently most of the other fixes and recommendation should suffice some of the risks of these devices. Below is the list of such devices –

Thales Air Traffic Control Systems (Models: TopSky ATC & Eurocat-C)
Thales IFE (In-Flight Entertainment) System (Model: Thales TopSeries i5000)
Thales IFE (In-Flight Entertainment) System (Model: Thales TopSeries AVANT)
Garmin G1000 Integrated Flight Deck (Model: Garmin G1000)
Frequentis VCS (Voice Communication System) (Model: Frequentis VCS 3020X)

Product/Vendor	Risk	Risk ID	Vulnerability	CVSS Severity	Mitigation
Hikvision Surveillance Cameras (Model: DS-2CD2xxx Series)	Improper authentication	R-001	**CVE-2017-7923** (NVD, 2017)	8.8	Update the firmware to V5.4.5 build 170123 or later (CISA, 2017)
		R-002	**CVE-2017-7921** (NVD, 2017)	10	
Honeywell Building Management Systems (Models: Honeywell XL Web II & Honeywell EBI R500)	Improper permission and authentication handling	R-003	**CVE-2017-5143** (NVD, 2017)	8.6	1. Move all possible subnets to internal to reduce the exposure to internet. 2. Use VPN for exposed subnets. 3. Move all the subnets behind Firewall and isolate them from other subnets 4. Update firmware to V.3.04.05.05 (CISA, 2018)
		R-004	**CVE-2017-5142** (NVD, 2017)	9.1	
		R-005	**CVE-2017-5141** (NVD, 2017)	6	
	Password stored in clear text	R-006	**CVE-2017-5140** (NVD, 2017)	9.8	
		R-007	**CVE-2017-5139** (NVD, 2017)	9.8	
	Remote access	R-008	**CVE-2015-0984** (NVD, 2015)	10	
	Cross-site scripting (XSS)	R-009	**CVE-2014-3110** (NVD, 2014)	4.3	
Garrett Metal Detectors (Models: Garrett PD 6500i & Garrett Multi Zone)	Buffer overflow	R-010	**CVE-2021-21907** (NVD, 2021)	4.9	Garrett have already released patch for the firmware update. It is recommended to update the firmware to latest version. (CISCO Talos, 2021)
		R-011	**CVE-2021-21906** (NVD, 2021)	7.2	
		R-012	**CVE-2021-21904** (NVD, 2021)	7.2	
		R-013	**CVE-2021-21903** (NVD, 2021)	9.8	
		R-014	**CVE-2021-21901** (NVD, 2021)	8.8	
	Directory traversal	R-015	**CVE-2021-21905** (NVD, 2021)	7.2	
	An authentication bypass	R-016	**CVE-2021-21902** (NVD, 2021)	8.1	

Axis Communications Network Cameras (Models: Axis Q6032-E & Axis M3005-V)	Remote code execution	R-017	**CVE-2022-23410** (NVD, 2022)	7.8	1. NCCST recommends to deploy strong IDS/IPS solutions and move the network behind a firewall. 2. Also, it is recommended to patch the systems to latest firmware versions (version 4.18.0). (Axis, 2018)
	Memory Corruption	R-018	**CVE-2018-10664** (NVD, 2018)	7.5	
	Incorrect Size Calculation	R-019	**CVE-2018-10663** (NVD, 2018)	7.5	
	Exposed Insecure Interface	R-020	**CVE-2018-10662** (NVD, 2018)	9.8	
	Bypass of access control	R-021	**CVE-2018-10661** (NVD, 2018)	9.8	
	Shell Command Injection	R-022	**CVE-2018-10660** (NVD, 2018)	9.8	
	Memory corruption issue	R-023	**CVE-2018-10659** (NVD, 2018)	7.5	
		R-024	**CVE-2018-10658** (NVD, 2018)	7.5	
Zebra ZXP Series 9 Card Printers (Model: ZXP Series 9)	Unrestricted end-user access to front panel options	R-025	**CVE-2019-10960** (NVD, 2019)	7.5	1. Minimize network exposure. 2. Use VPN and firewall when the remote access is required. (CISA, 2019)

2.3 Risk Register

Risk Register

Risk ID	Date	Risk Owner	Asset	Description	Impact	Likelihood	Severity
R-001	12-7-24	Airport security team	Hikvision - DS-2CD2xxx	Improper authentication vulnerability	Very high	High	High
R-002	12-7-24	Airport security team	Hikvision - DS-2CD2xxx	Improper authentication vulnerability	Very high	High	Very high
R-003	12-7-24	Airport security team	Honeywell - XL Web II	Improper permission and authentication handling	Very high	Low	High
R-004	12-7-24	Airport security team	Honeywell - XL Web II	Improper permission and authentication handling	Very high	Very high	Very high
R-005	12-7-24	Airport security team	Honeywell - XL Web II	Improper permission and authentication handling	Very high	Low	Medium
R-006	12-7-24	Airport security team	Honeywell - XL Web II	Password stored in clear text	Very high	High	Very high
R-007	12-7-24	Airport security team	Honeywell - XL Web II	Password stored in clear text	Very high	High	Very high
R-008	12-7-24	Airport security team	Honeywell - XL Web II	Remote access	Very high	Very high	Very high
R-009	12-7-24	Airport security team	Honeywell - XL Web II	Cross-site scripting (XSS) vulnerability	High	Low	Medium
R-010	12-7-24	Passenger safety team	Garrett Metal Detectors	Buffer overflow vulnerability	Medium	Medium	Medium
R-011	12-7-24	Passenger safety team	Garrett Metal Detectors	Buffer overflow vulnerability	Medium	High	High
R-012	12-7-24	Passenger safety team	Garrett Metal Detectors	Buffer overflow vulnerability	Medium	High	High
R-013	12-7-24	Passenger safety team	Garrett Metal Detectors	Buffer overflow vulnerability	Medium	Very high	Very high
R-014	12-7-24	Passenger safety team	Garrett Metal Detectors	Buffer overflow vulnerability	Medium	High	High

R-015	12-7-24	Passenger safety team	Garrett Metal Detectors	Directory traversal vulnerability	Very high	Low	High
R-016	12-7-24	Passenger safety team	Garrett Metal Detectors	An authentication bypass vulnerability	Very high	Medium	High
R-017	12-7-24	Airport security team	Axis IP cameras	Remote code execution	Very high	Low	High
R-018	12-7-24	Airport security team	Axis IP cameras	Memory Corruption	High	High	High
R-019	12-7-24	Airport security team	Axis IP cameras	Incorrect Size Calculation	Medium	High	High
R-020	12-7-24	Airport security team	Axis IP cameras	Exposed Insecure Interface	Very high	High	Very high
R-021	12-7-24	Airport security team	Axis IP cameras	Bypass of access control	Very high	Very high	Very high
R-022	12-7-24	Airport security team	Axis IP cameras	Shell Command Injection	Very high	High	Very high
R-023	12-7-24	Airport security team	Axis IP cameras	Memory corruption issue	Medium	Very high	High
R-024	12-7-24	Airport security team	Axis IP cameras		Medium	High	High
R-025	12-7-24	Admin office	Zebra Card Printers	Unrestricted end-user access to front panel options	Very high	Medium	High

2.4 Severe risks analysis

Risk 1: Improper authentication

Affected devices:

1. Hikvision Surveillance Cameras (Model: DS-2CD2xxx Series)
2. Honeywell Building Management Systems (Models: Honeywell XL Web II)
3. Garrett Metal Detectors (Models: Garrett PD 6500i & Garrett Multi Zone)

Identified vulnerabilities:

- CVE-2017-7923
- CVE-2017-7921
- CVE-2017-5143
- CVE-2017-5142
- CVE-2017-5141
- CVE-2021-21902

Impact analysis:

The impact of improper authentication vulnerabilities for the mentioned devices could cause some serious issue such as:

- Data Breaches:
  Attackers can gain unauthorized access to sensitive data, such as surveillance footage, building control systems, and potentially even passenger information. This could lead to data breaches.

- System Disruption:
  Compromised devices can be manipulated to disrupt critical operations and day to day operations of the airport.

- Surveillance Systems:
  Disrupting video feeds, modifying recordings, or using cameras for surveillance of unauthorized areas.

- Building Management Systems:
  Disrupting temperature control, access control, fire suppression systems, or other critical building functions.

- Metal Detectors:
  Manipulating detector settings, bypassing security checks, or even triggering false alarms, creating chaos and security risks.

- Safety and Security Risks:
  In an airport environment, these disruptions can pose significant safety and security risks to passengers, staff, and aircraft.

- Reputational Damage:
  Data breaches and service disruptions can severely damage the airport's reputation and erode public trust.

Risk 2: Password stored in clear text

Affected devices:

1. Honeywell Building Management Systems (Models: Honeywell XL Web II & Honeywell EBI R500)

Identified vulnerabilities:

- CVE-2017-5140
- CVE-2017-5139

Impact analysis:

This is a very serious risk as attacker can get all the credentials of the users and many of the systems can be further compromised with this access. This could lead to:

- Unauthorized Access:
  Attackers can easily gain access to the system by obtaining the stored credentials.

- System Control:
  This access allows attackers to manipulate building systems, including:
  - HVAC control: Disrupting temperature and humidity levels, potentially impacting occupant comfort and safety.
  - Access control: Manipulating door locks and security systems, compromising building security.
  - Fire suppression systems: Potentially interfering with fire safety systems.
  - Energy management systems: Disrupting energy efficiency measures and increasing operational costs.

- Data Theft:
  Attackers may be able to access and steal sensitive data stored within the building management system, such as occupant schedules, maintenance records, and potentially even personal information.

- Service Disruption:
  Malicious activities can cause significant disruptions to building operations, impacting business continuity and potentially leading to financial losses.

Risk 3: Remote access

Affected devices:

2. Honeywell Building Management Systems (Models: Honeywell XL Web II & Honeywell EBI R500)

Identified vulnerabilities:

- CVE-2015-0984

Impact analysis:

Impact of this risk is similar to the Risk 2 mentioned above.

- Unauthorized System Control:
  Attackers can exploit these vulnerabilities to gain remote access to the system, allowing them to manipulate building systems without physical presence.

- Disruption of Critical Functions:
  This could lead to disruptions of HVAC controls, fire and electric safety systems and access control disruptions.

- Data Theft and Manipulation:
  Attackers could potentially access and steal sensitive data stored within the building management system, or even manipulate data for malicious purposes.

3.5 Severe vulnerability analysis

Vulnerability 1: CVE-2017-7921 (NVD, 2017)

Affected device: Hikvision Surveillance Cameras (Model: DS-2CD2xxx Series)

CVSS v3 score: 10 Critical

Vulnerability Type: Improper Authentication

NVD Published Date: 05/05/2017

Description:

CVE-2017-7921 is a vulnerability affecting Hikvision IP cameras installed on the airport. It involves an improper authentication issue that allows an attacker to potentially escalate their privileges on the device. This could also enable them to gain unauthorized access to sensitive information or control the camera's functions.

Impact:

Potential privilege escalation, unauthorized access, and control of camera functions.

Mitigation:

Vendor has already released security patch for the firmware, updating the firmware to V5.4.5 build 170123 or later should fix the issue.

Vulnerability 2: CVE-2015-0984 (NVD, 2015)

Affected device: Honeywell Building Management Systems (Models: Honeywell XL Web II)

CVSS v3 score: 10 Critical

Vulnerability Type: Remote access

NVD Published Date: 03/30/2015

Description:

CVE-2015-0984 affects older Honeywell controllers. It allows an attacker to potentially read files outside the intended directory, potentially exposing sensitive information.

Impact:

- Remote attackers could potentially exploit this vulnerability to read files outside the intended directory on the affected devices.
- This could potentially lead to the disclosure of sensitive information, such as system configuration files, credentials, or even firmware.

Mitigation:

- Updating Excel Web Linux to version 2.04.01 and programing tool CARE version 10.02 or later
- Network isolation and use of VPN for remote access.
- Also, use firewalls and WAF for further safety.

Vulnerability 3: CVE-2017-5140 (NVD, 2017)

Affected device: Honeywell Building Management Systems (Models: Honeywell XL Web II)

CVSS v3 score: 9.8 Critical

Vulnerability Type: Credential mismanagement

NVD Published Date: 03/30/2015

Description:

CVE-2017-5140 is another vulnerability in older Honeywell XL Web II controllers where passwords are stored in plain text making them easily accessible to anyone who gains access to the system.

Impact:

- Remote attackers could potentially exploit this vulnerability to read files outside the intended directory on the affected devices.
- This could potentially lead to the disclosure of sensitive information, such as system configuration files, credentials, or even firmware.

Mitigation:

- Update the firmware to v3.04.05.05
- Network exposure minimization
- Move the internet exposed networks behind firewall.
- Implementation of IDS and IPS
- Use VPN

4 Recommendations

Recommendations	Justification
Prioritize Patch Management	Many of these risks can be mitigated by updating the devices to latest firmware versions
Implement and Enforce Strong Authentication	Many of the security controls can be of no use if the password is easy to guess. So, a strong password policy is required.
Limit the network exposure to internet	Reducing the exposure to internet reduces the attack surface to the threats. Implementing proxies and diverting traffic through it can help with this situation.
Network Segmentation	Dividing the networks into multiple subnets reduces the damage to a specific network.
VPN setup	VPN can help with the traffic coming from various sites or devices by moving it through a virtual tunnel. This makes various attacks like MITM or network tapping.
Intrusion Detection and Prevention Systems (IDPS)	IDPS scans for incoming traffic and can help flag or stop packets that are suspicious.
Implement Firewalls and WAF	Firewalls can help with the network level traffic filtering and WAF can be used for web traffic.
Implement Least Privilege Access Controls	This method reduces the risk when some credentials are compromised. Limiting the permission and privileges to required roles makes the job difficult for the attacker.
Data Encryption	All data and passwords should be encrypted to avoid data exfiltration.
Employee Training and Awareness	Humans are always the weakest link in a system. Training the employees to identify the suspicious mails and reported them to correct can improve the overall security posture.

Top recommendations:

1. Patching:

There are always some vulnerabilities left in any product. Some of these are identified by various teams on regular basis which can be fixed easily. Some vulnerably are not known to the vendor which are called as zero day exploits.

These vulnerabilities, if exploited, could allow attackers to gain unauthorized access to sensitive data like passenger information, flight schedules, and even control critical infrastructure such as air traffic control systems and can cause serious disruptions. Timely patching minimizes the risk of successful cyberattacks, ensuring the safety and security of all airport operations and passengers

2. Network security measure – Firewalls and IDPS:

Implementing firewalls and IDPS is crucial for airport security to safeguard sensitive data, maintain operational continuity, and protect passenger safety. Firewalls act as the first line of defense, controlling network traffic by filtering incoming and outgoing traffic based on predefined rules. This prevents unauthorized access to critical systems and data.

IDPS systems actively monitor network activity for malicious patterns and anomalies. It helps by detecting potential threats like intrusions, malware, and data exfiltration attempts. By promptly identifying and responding to these threats, IDPS can helps mitigate risks and prevent significant disruptions to airport operations.

3. Employee training and awareness

Humans are considered as weakest link in a security chain. It can be anything from phishing mails sent to certain employees to spear phishing some high ranking individuals. Employee training and awareness programs are fundamental to security. By educating employees about cybersecurity threats, best practices for data handling and the importance of reporting suspicious activity, airports can significantly reduce the risk of human error and social engineering attacks.

References

Axis, 2018. *Advisory_ACV-128401*. [Online]
Available at: https://www.axis.com/files/faq/Advisory_ACV-128401.pdf
[Accessed 12 2024].

CISA, 2017. *Hikvision Cameras*. [Online]
Available at: https://www.cisa.gov/news-events/ics-advisories/icsa-17-124-01
[Accessed 12 2024].

CISA, 2018. *Honeywell FALCON XLWeb Controllers Vulnerabilities*. [Online]
Available at: https://www.cisa.gov/news-events/ics-advisories/icsa-14-175-01
[Accessed 12 2024].

CISA, 2019. *Zebra Industrial Printers*. [Online]
Available at: https://www.cisa.gov/news-events/ics-advisories/icsa-19-232-01
[Accessed 12 2024].

CISCO Talos, 2021. *TALOS-2021-1354*. [Online]
Available at: https://talosintelligence.com/vulnerability_reports/TALOS-2021-1354
[Accessed 12 2024].

NVD, 2014. *CVE-2014-3110*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2014-3110
[Accessed 12 2024].

NVD, 2015. *CVE-2015-0984*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2015-0984
[Accessed 12 2024].

NVD, 2017. *CVE-2017-5139*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-5139
[Accessed 12 2024].

NVD, 2017. *CVE-2017-5140*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-5140
[Accessed 12 2024].

NVD, 2017. *CVE-2017-5141*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-5141
[Accessed 12 2024].

NVD, 2017. *CVE-2017-5142*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-5142
[Accessed 12 2024].

NVD, 2017. *CVE-2017-5143*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-5143
[Accessed 12 2024].

NVD, 2017. *CVE-2017-7921*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-7921
[Accessed 12 2024].

NVD, 2017. *CVE-2017-7921*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-7921
[Accessed 12 2024].

NVD, 2017. *CVE-2017-7923*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-7923
[Accessed 12 2024].

NVD, 2018. *CVE-2018-10658*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2018-10658
[Accessed 12 2024].

NVD, 2018. *CVE-2018-10659*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2018-10659
[Accessed 12 2024].

NVD, 2018. *CVE-2018-10660*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2018-10660
[Accessed 12 2024].

NVD, 2018. *CVE-2018-10661*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2018-10661
[Accessed 12 2024].

NVD, 2018. *CVE-2018-10662*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2018-10662
[Accessed 12 2024].

NVD, 2018. *CVE-2018-10663*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2018-10663
[Accessed 12 2024].

NVD, 2018. *CVE-2018-10664*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2018-10664
[Accessed 12 2024].

NVD, 2019. *CVE-2019-10960*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2019-10960
[Accessed 12 2024].

NVD, 2021. *CVE-2021-21901*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21901
[Accessed 12 2024].

NVD, 2021. *CVE-2021-21902*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21902
[Accessed 12 2024].

NVD, 2021. *CVE-2021-21903*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21903
[Accessed 12 2024].

NVD, 2021. *CVE-2021-21904*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21904
[Accessed 12 2024].

NVD, 2021. *CVE-2021-21905*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21905
[Accessed 12 2024].

NVD, 2021. *CVE-2021-21906*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21906
[Accessed 12 2024].

NVD, 2021. *CVE-2021-21907*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21907
[Accessed 12 2024].

NVD, 2022. *CVE-2022-23410*. [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2022-23410
[Accessed 12 2024].