CR Vulnerability Disclosures

Reviewing the Security of the EKEN Smart Video Doorbell Camera Wireless with Chime Ringer and the Tuck Sharkpop Doorbell Camera Wireless

BY GLEN ROCKFORD, STEVE BLAIR AND DAVID DELLAROCCA

FEBRUARY 29, 2004

CR Consumer Reports®

EKEN Smart Video Doorbell Camera Wireless with Chime Ringer Vulnerability Disclosure

January 2024

Executive Summary

In January of 2024, Consumer Reports reviewed the security of the Eken Smart Video Doorbell Camera Wireless with Chime Ringer (Firmware: 2.8.1 , App version: 2.8.2 (Eken Utilizes the Aiwit Application) The findings below were observed during testing:

1: The user's public facing IP is broadcast over the internet and network unencrypted. (Medium Risk)
2: Unauthenticated Access to JPEG via Server URL in [Vendor/Service] (High Risk)
3: The Users Local SSID is broadcast over the internet and network unencrypted. (Medium Risk)
4: Unauthorized Ownership of Video Doorbell (Aiwit Application) (High Risk)

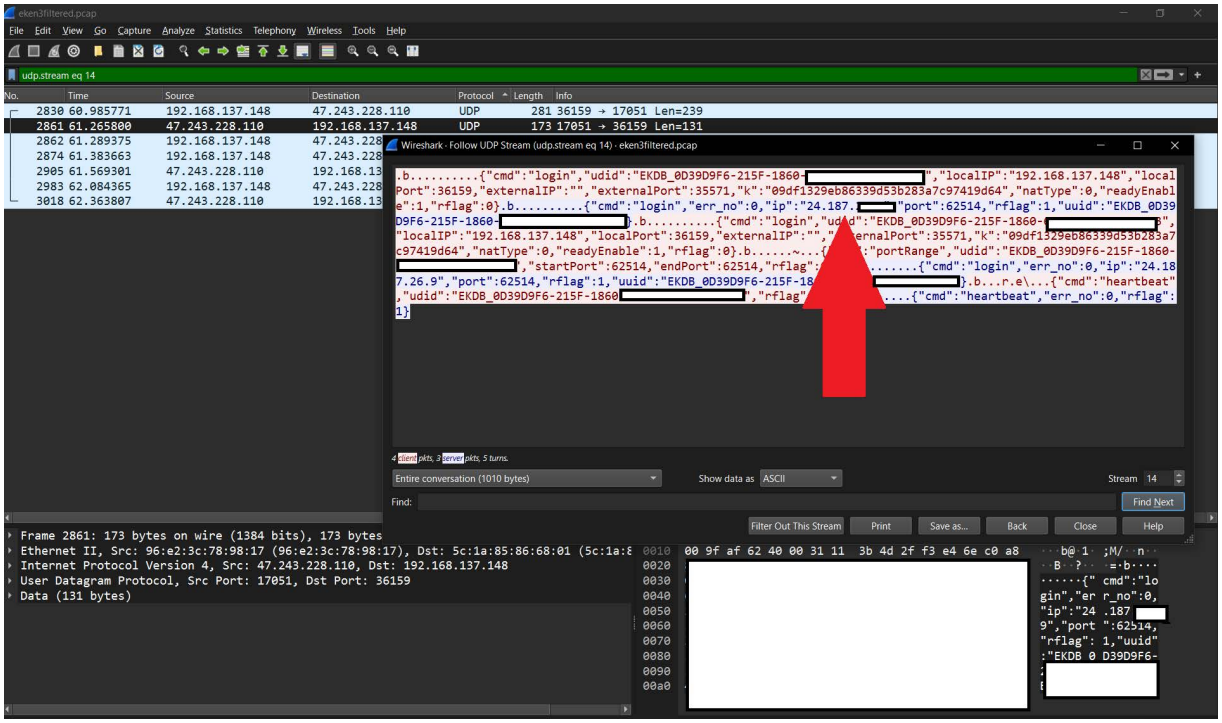
Finding Number	Category	Risk	Exploitability	Impact
1	Data Exposure	Medium	Medium	Medium
2	Broken Access Control	High	High	High
3	Data Exposure	Medium	Medium	Medium
4	Unauthorized Ownership/Lack of Factory Reset Controls	High	High	High

Detailed Findings

Finding 1: The user's public facing IP is broadcast over the internet and network unencrypted.

IP addresses are considered to be Personally Identifiable Information (PII) by multiple authorities including the CCPA (CCPA 1798.148 section V, 1A). Transmission of PII in cleartext does not meet best practices.

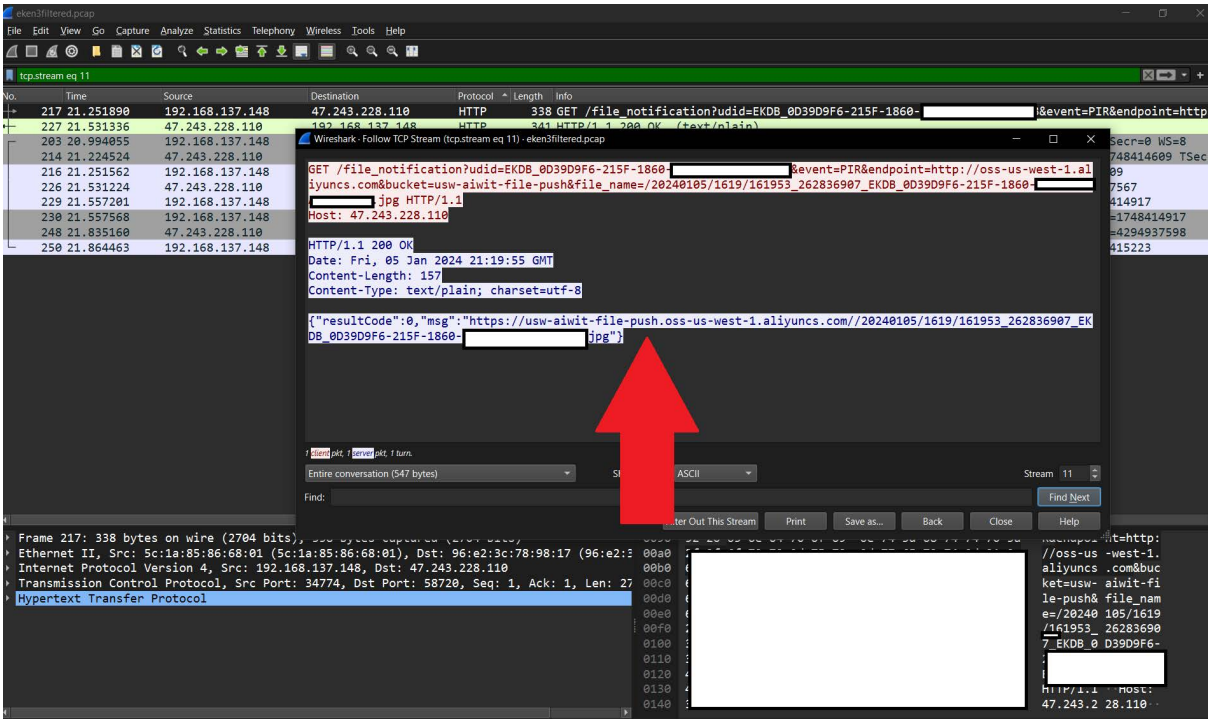
Once a user connects the device to their network, their public facing IP address is seen in the network traffic of the Wireless Security Camera in clear text (see screenshots below). (24.187.**).Testers External IP partially obscured in network capture image.



Finding 2: Unauthenticated Access to JPEG via Server URL in [Vendor/Service]

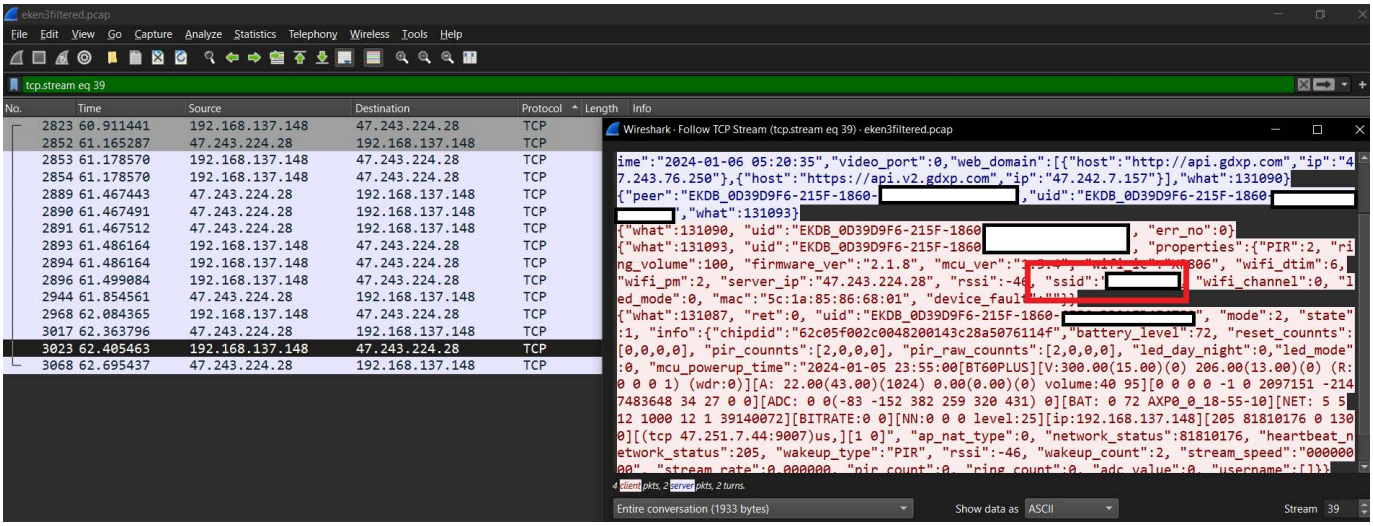
During network packet analysis, it was observed that a server is broadcasting a JPEG file without proper access controls; it is possible to intercept and download the JPEG file without the need for authentication. Within the captured packets, we identified the server's response containing the JPEG file.We were then able to extract the URL from the response, copy the extracted server URL from the log, open a web browser and paste the copied URL into the address bar, and the server fulfills the HTTP request without the need for authentication, allowing the unauthorized download of the JPEG file specified in the URL, By mimicking an IDOR (Insecure Direct Object Reference) Vulnerability. The server fulfills the HTTP request,

allowing the unauthorized download of the JPEG file specified in the URL. This poses a potential risk of unauthorized access to sensitive content. (See Screenshot Below)



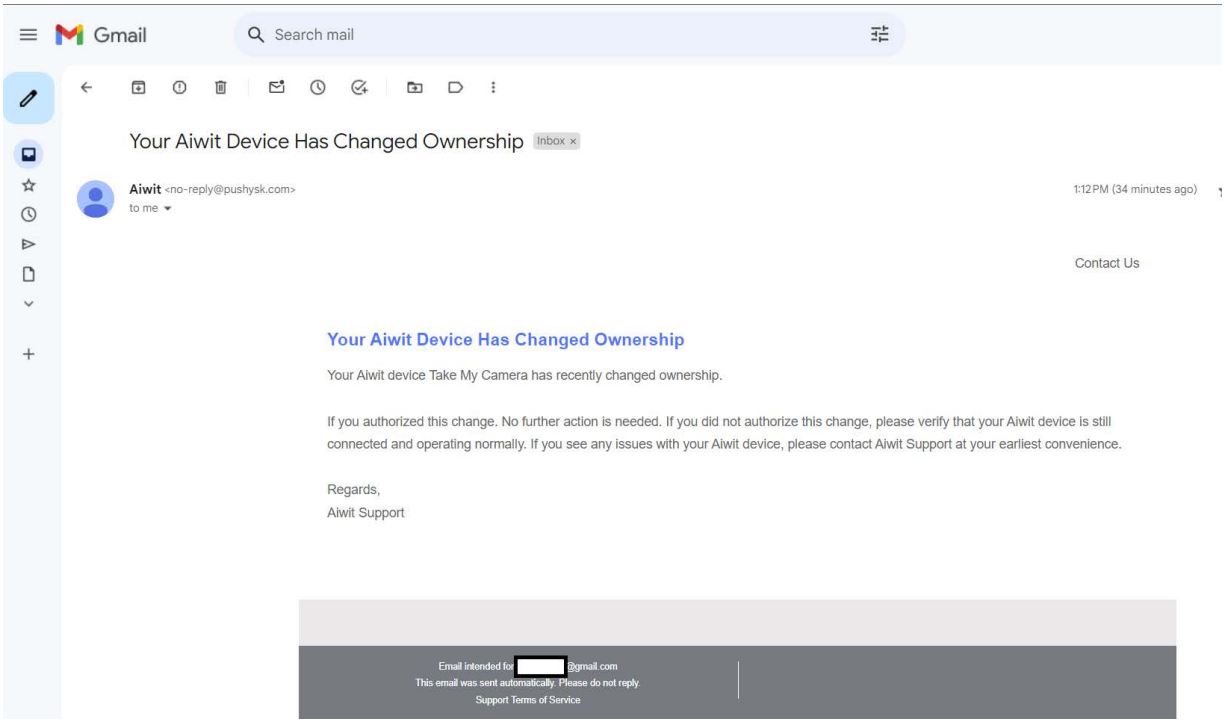
Finding 3: The Users Local SSID is broadcast over the internet and network unencrypted.

During network packet analysis, it was observed that the local SSID (Service Set Identifier) is being broadcasted unencrypted and displayed in clear text during network communication. Exposure of the SSID in clear text poses a risk to user privacy and network security, increases the risk of unauthorized access to the network, potentially leading to unauthorized data access or manipulation. (See Screenshot Below)

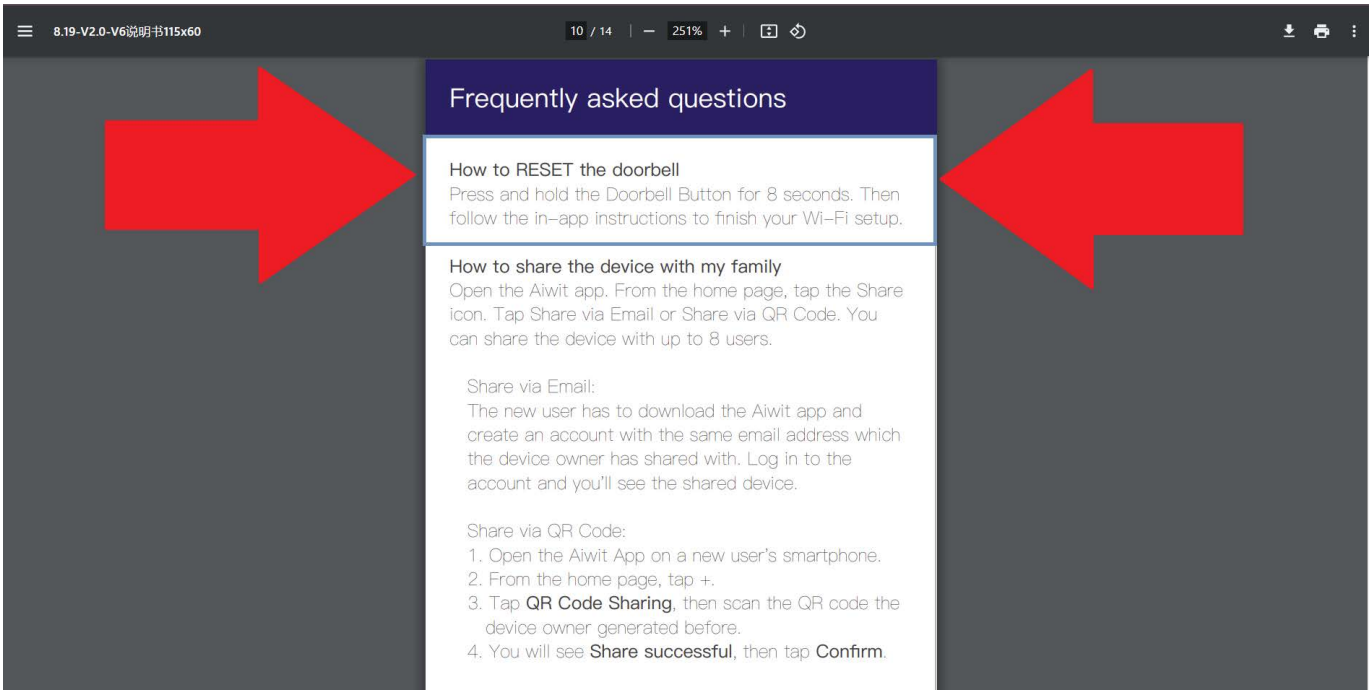


Finding 4: Unauthorized Ownership of Video Doorbell (Aiwit Application)

During the course of testing the Eken video doorbell it was discovered that it is very easy for an unauthorized malicious actor to take full control of the video doorbell. Since this video doorbell does not have factory reset controls, an outside actor can exploit this to take ownership of the video doorbell. A malicious actor can put the doorbell into pairing mode simply by holding down the doorbell button for 8 seconds. The malicious user, who has simply downloaded the Aiwit app and has created their own account, can now scan the QR code generated by the app (The QR code is scanned simply by holding their mobile device screen up to the camera on the video doorbell). This QR code allows the video doorbell to connect to a different network (i.e. mobile hotspot set up by the malicious user). By scanning the QR code generated by the app for adding the video doorbell, they can successfully add the video doorbell to their account, gain control over a device that was originally associated with the homeowner's user account. The user who loses access to the doorbell will receive an email alerting them that ownership of their camera has changed. (See Screenshot Below). This is good, but until the owner of the video doorbell reads this email and can take the steps to reclaim it, the unauthorized malicious actor has full access to view and hear all activity picked up by the video doorbell.



Instructions to reset doorbell found here: Eken Manual Tester was unable to find any further instructions on factory resetting the doorbell. The only instructions found enable the device to enter pairing mode. (See Screenshots Below)



Possible Remediations

- **Finding #1**
  - Don't store or transmit sensitive data unnecessarily.
  - Encrypt all sensitive data at rest, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management.
  - Encrypt all data in transit with secure protocols and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
  - Independent verification of the effectiveness of configuration and settings is ideal.

- **Finding #2**
  - Encrypt all sensitive data in transit, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management for the transmission of sensitive data from the devices, ensuring that the content remains confidential and protected from unauthorized access during transit.
  - Implement stringent access controls on the server, requiring authentication. Such as; access token-based authentication mechanisms requiring valid tokens to control access to the server.

- **Finding #3**
  - Don't store or transmit sensitive data unnecessarily.
  - Encrypt all sensitive data at rest, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management.

- Encrypt all data in transit with secure protocols and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
- Independent verification of the effectiveness of configuration and settings is ideal.

- **Finding #4**
  - Secure Reset Mechanism: Develop and implement a secure factory reset mechanism that includes additional verification steps, making it resistant to unauthorized attempts.
  - Device Identity Verification: Integrate device identity verification measures during the factory reset process, ensuring that only authorized users can initiate and complete the reset procedure.
  - Multi-Factor Authentication (MFA): Enforce multi-factor authentication during the setup process to add an extra layer of security.
  - Role-Based Access Control (RBAC): Implement RBAC to manage and restrict user access rights, ensuring that only authorized individuals have the necessary permissions to configure and control the video doorbell.

Tuck Sharkpop Doorbell Camera Wireless Vulnerability Disclosure

January 2024

Executive Summary

In January of 2024, Consumer Reports reviewed the security of the Tuck Sharkpop Doorbell Camera Wireless (Firmware: 2.8.1 , App version: 2.8.2 (Tuck Utilizes the Aiwit Application) The findings below were observed during testing:

1: The user's public facing IP is broadcast over the internet and network unencrypted. (Medium Risk)
2: Unauthenticated Access to JPEG via Server URL in [Vendor/Service] (High Risk)
3: The Users Local SSID is broadcast over the internet and network unencrypted. (Medium Risk)
4: Unauthorized Ownership of Video Doorbell (Aiwit Application) (High Risk)

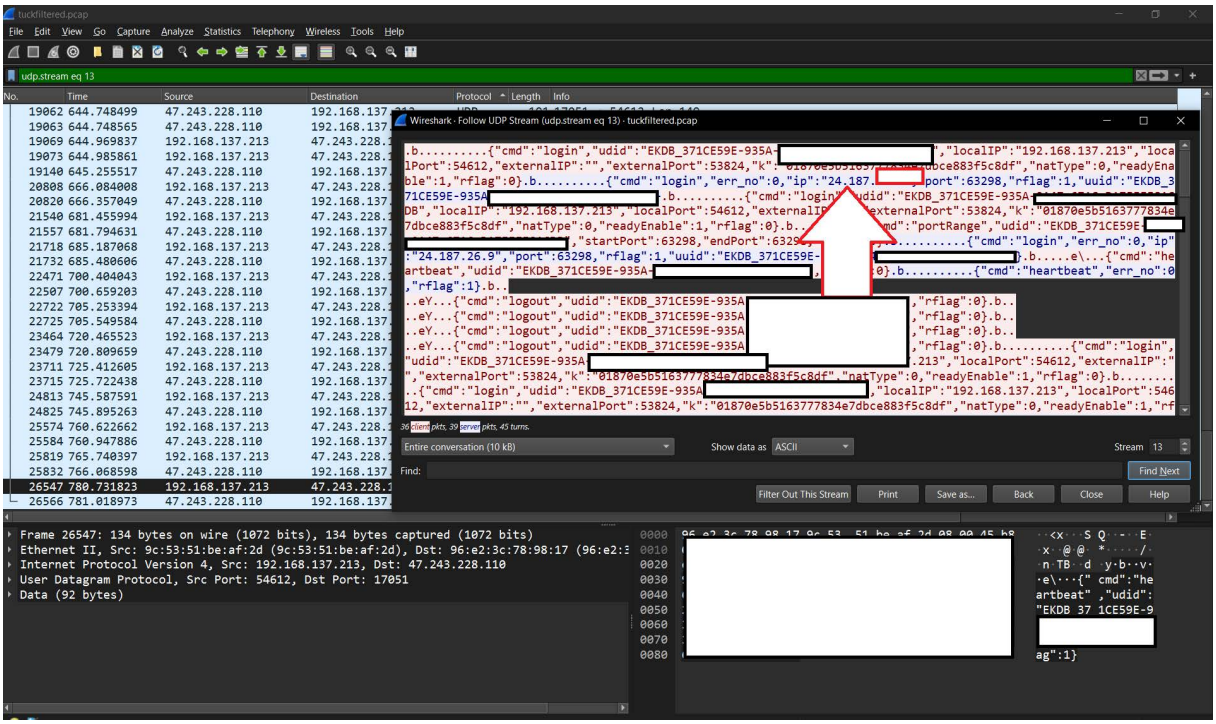
Finding Number	Category	Risk	Exploitability	Impact
1	Data Exposure	Medium	Medium	Medium
2	Broken Access Control	High	High	High
3	Data Exposure	Medium	Medium	Medium
4	Unauthorized Ownership/Lack of Factory Reset Controls	High	High	High

Detailed Findings

Finding 1: The user's public facing IP is broadcast over the internet and network unencrypted.

IP addresses are considered to be Personally Identifiable Information (PII) by multiple authorities including the CCPA (CCPA 1798.148 section V, 1A). Transmission of PII in cleartext does not meet best practices.

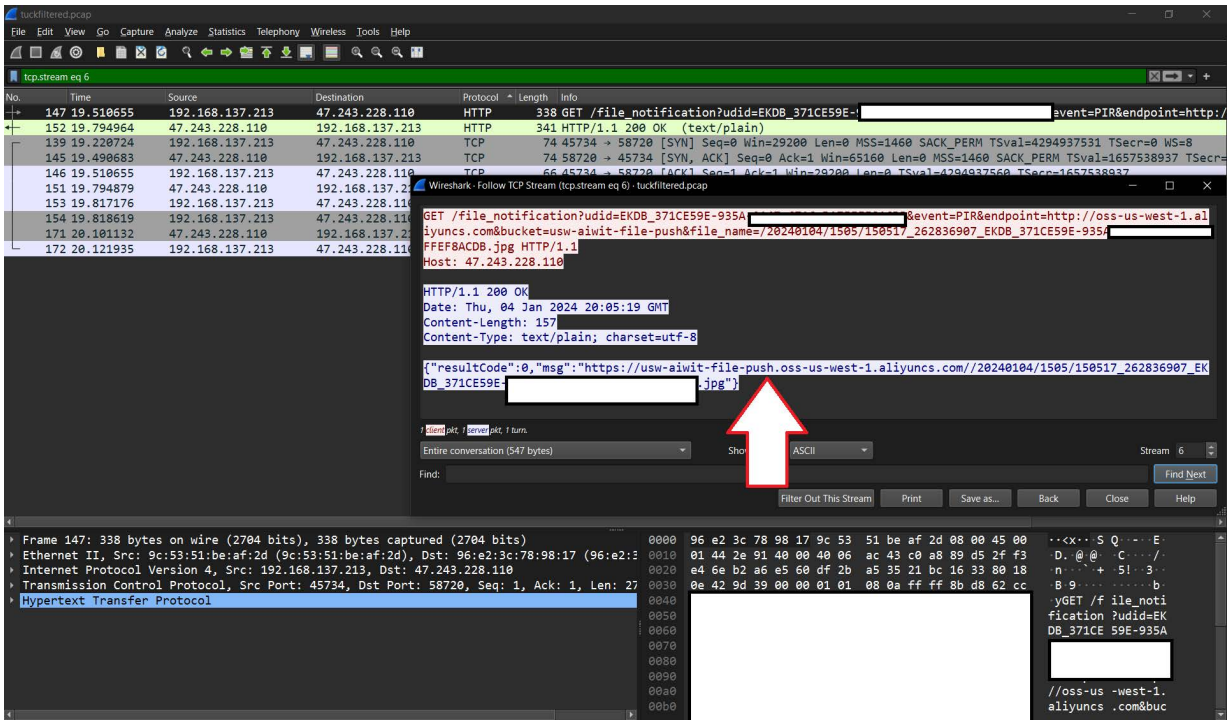
Once a user connects the device to their network, their public facing IP address is seen in the network traffic of the Wireless Security Camera in clear text (see screenshots below). (24.187.**).Testers External IP partially obscured in network capture image.



Finding 2: Unauthenticated Access to JPEG via Server URL in [Vendor/Service]

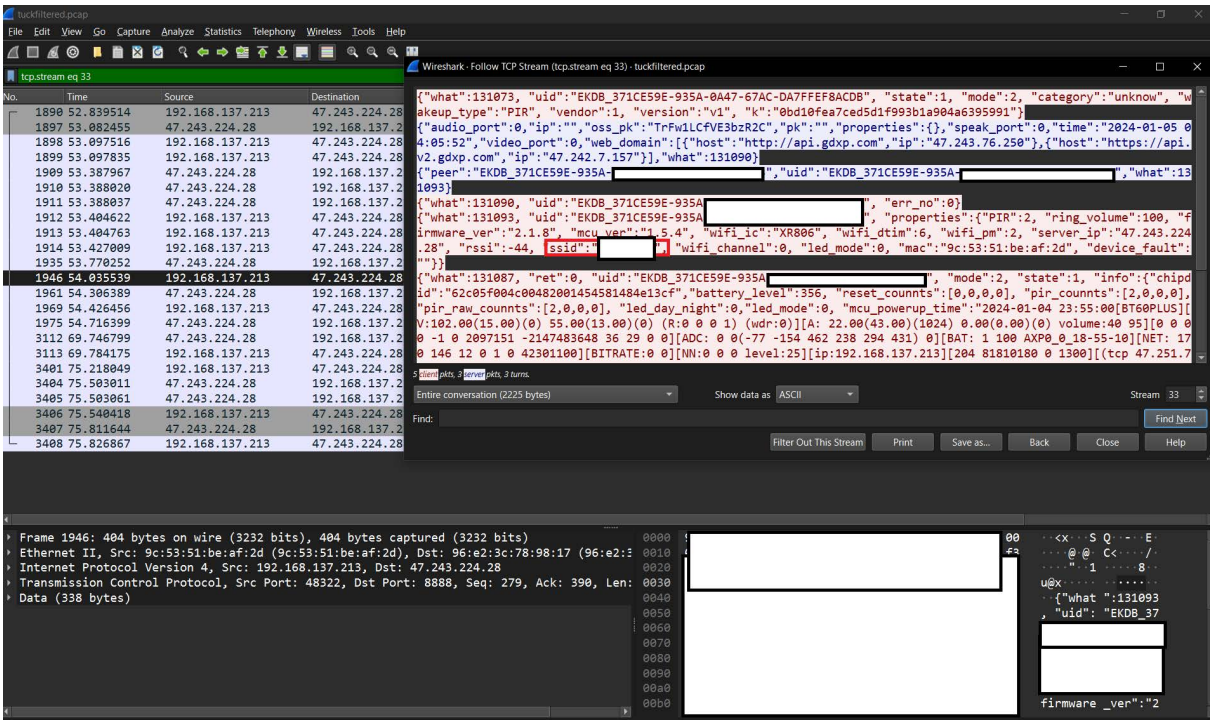
During network packet analysis, it was observed that a server is broadcasting a JPEG file without proper access controls; it is possible to intercept and download the JPEG file without the need for authentication. Within the captured packets, we identified the server's response containing the JPEG file.We were then able to extract the URL from the response, copy the extracted server URL from the log, open a web browser and paste the copied URL into the address bar, and the server fulfills the HTTP request without the need for authentication, allowing the unauthorized download of the JPEG file specified in the URL, By mimicking an

IDOR (Insecure Direct Object Reference) Vulnerability. The server fulfills the HTTP request, allowing the unauthorized download of the JPEG file specified in the URL. This poses a potential risk of unauthorized access to sensitive content. (See Screenshot Below)



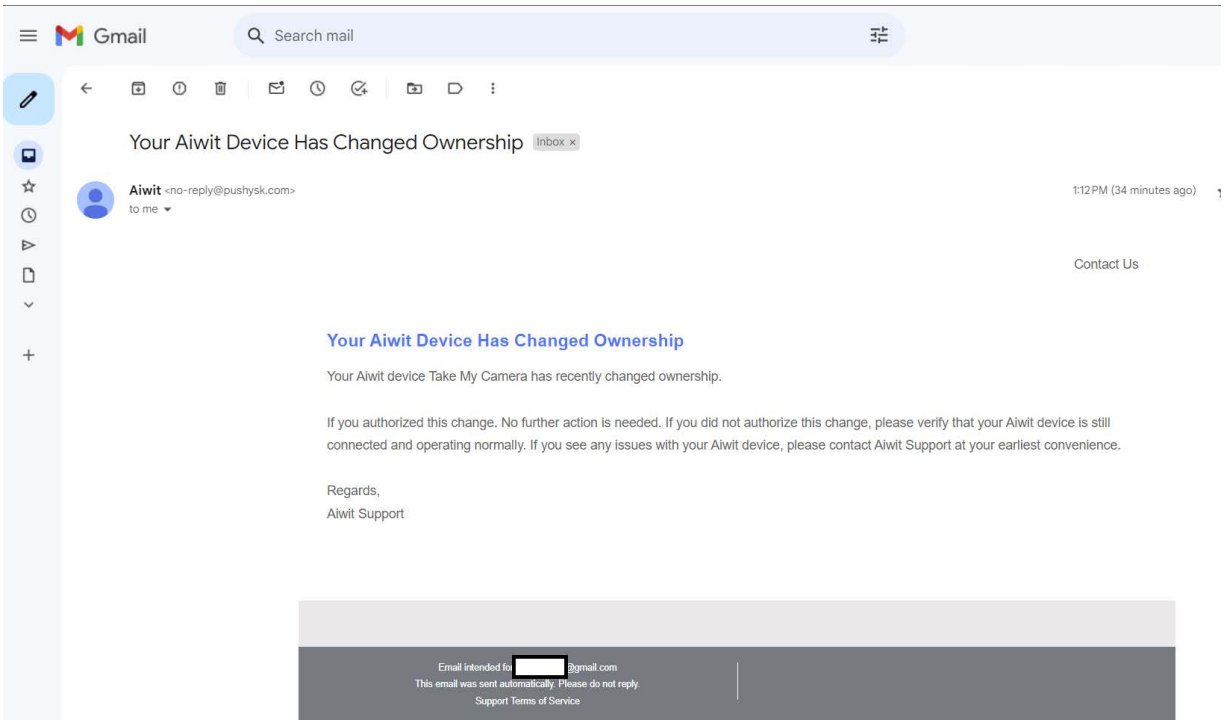
Finding 3: The Users Local SSID is broadcast over the internet and network unencrypted.

During network packet analysis, it was observed that the local SSID (Service Set Identifier) is being broadcasted unencrypted and displayed in clear text during network communication. Exposure of the SSID in clear text poses a risk to user privacy and network security, increases the risk of unauthorized access to the network, potentially leading to unauthorized data access or manipulation. (See Screenshot Below)



Finding 4: Unauthorized Ownership of Video Doorbell (Aiwit Application)

During the course of testing the Tuck video doorbell it was discovered that it is very easy for an unauthorized malicious actor to take full control of the video doorbell. Since this video doorbell does not have factory reset controls, an outside actor can exploit this to take ownership of the video doorbell. A malicious actor can put the doorbell into pairing mode simply by holding down the doorbell button for 8 seconds. The malicious user, who has simply downloaded the Aiwit app and has created their own account, can now scan the QR code generated by the app (The QR code is scanned simply by holding their mobile device screen up to the camera on the video doorbell). This QR code allows the video doorbell to connect to a different network (i.e. mobile hotspot set up by the malicious user). By scanning the QR code generated by the app for adding the video doorbell, they can successfully add the video doorbell to their account, gain control over a device that was originally associated with the homeowner's user account. The user who loses access to the doorbell will receive an email alerting them that ownership of their camera has changed. (See Screenshot Below). This is good, but until the owner of the video doorbell reads this email and can take the steps to reclaim it, the unauthorized malicious actor has full access to view and hear all activity picked up by the video doorbell.



Possible Remediations

- **Finding #1**
  - Don’t store or transmit sensitive data unnecessarily.
  - Encrypt all sensitive data at rest, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management.
  - Encrypt all data in transit with secure protocols and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
  - Independent verification of the effectiveness of configuration and settings is ideal.

- **Finding #2**
  - Encrypt all sensitive data in transit, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management for the transmission of sensitive data from the devices, ensuring that the content remains confidential and protected from unauthorized access during transit.
  - Implement stringent access controls on the server, requiring authentication. Such as; access token-based authentication mechanisms requiring valid tokens to control access to the server.

- **Finding #3**
  - Don't store or transmit sensitive data unnecessarily.
  - Encrypt all sensitive data at rest, ensuring up-to-date and strong industry standard algorithms, protocols and keys are in place. Use proper key management.
  - Encrypt all data in transit with secure protocols and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
  - Independent verification of the effectiveness of configuration and settings is ideal.

- **Finding #4**
  - Secure Reset Mechanism: Develop and implement a secure factory reset mechanism that includes additional verification steps, making it resistant to unauthorized attempts.
  - Device Identity Verification: Integrate device identity verification measures during the factory reset process, ensuring that only authorized users can initiate and complete the reset procedure.
  - Multi-Factor Authentication (MFA): Enforce multi-factor authentication during the setup process to add an extra layer of security.
  - Role-Based Access Control (RBAC): Implement RBAC to manage and restrict user access rights, ensuring that only authorized individuals have the necessary permissions to configure and control the video doorbell.

External Audience Protocol (EAP) - Video Doorbells Privacy Testing

Purpose of this document:

This document is generated by the testing team to describe what tests are done in our evaluation of data privacy and security of Video Doorbells. Specifically, it refers to the relevant criteria and indicators from the Digital Standard that apply to this testing. It also provides an overview of our testing methodologies.

Who was this created for?

The primary audience for this document is Video Doorbell manufacturers, who are typically interested in understanding what our tests are looking for and what our ratings are based on.

Introduction

Video Doorbells are increasing in popularity due to dropping prices and more consumer interest. They provide users with access to video and audio footage, live or recorded, over the internet, which presents the possibility for this data to be accessed, stored, shared, bought, sold, and stolen. Therefore, the security and privacy of these Video Doorbell Cameras is a primary concern for consumers and Consumer Reports. Not only do we need to test the performance of Video Doorbells (e.g. clarity, convenience) but also make sure the Video Doorbell Camera is protecting the owner, not monitoring them.

Test Description

Products are tested in accordance with the following criteria/indicators of the Digital Standard (https://www.thedigitalstandard.org/).

Privacy

1. Data Control - I can see and control everything the company knows about me.
    a. Users can control the collection of their information.
    b. Users can delete their information.
    c. Users can control how their information is used to target advertising.
    d. Users can obtain a copy of their information.
    e. Clear explanations of how users can control their data.
    f. Privacy controls exist and are effective.
2. Data Share - Data sharing is reasonably scoped and transparent.

   a. The company only shares information with third parties as is reasonably necessary to deliver service to consumers.
   b. The company clearly discloses what user information it shares with whom.
   c. The company clearly discloses the types of third parties with which it shares user information.
   d. The company clearly discloses the names of third parties with which it shares user information.
   e. The company clearly discloses whether it shares user information with government or legal authorities.
   f. Third-party domains contacted by the product are named in the privacy policy.
3. Data Use - Data usage is consistent with the context of the relationship with the user and is transparent.
   a. The company puts limits on the use of my data that is consistent with the purpose for which the data is collected.
   b. The company explicitly discloses every way in which it uses my data.
4. Data Retention and Deletion - I know how long the company keeps my information.
   a. All user information is deleted after users terminate their accounts or remove service from a device.
   b. Disclosure of timeframe in which user information is deleted after users terminate their account.
   c. Disclosure of how long each type of user information is retained.
5. Data Collection - I know what user information this company is collecting and when.
   a. Disclosure of the type of user information collected.
   b. Disclosure of how user information is collected.
   c. The device gives clear indication (e.g., lit LED) when cameras and microphones are active.
6. Minimal Data Collection - The only information the company requests from me is what's needed to make the product or service work correctly.
   a. The user information collected is only that which is directly relevant and necessary for the service.
   b. The product still works when all permissions not relevant to the product's functionality are declined.
7. Privacy by Default - The default settings in this product prioritize my privacy; to give up privacy, I actually need to change the settings.
   a. Targeted advertising is off by default.
   b. User interface settings that are optimal for privacy are set by default.
8. Data benefits - Every piece of data I share brings me a benefit; it doesn't just help the company.
   a. The company clearly discloses its purpose for collecting each type of user information.
9. Data benefits - Every piece of data I share brings me a benefit; it doesn't just help the company.
   a. The company clearly discloses its purpose for collecting each type of user information.

10. Terms of Service and Privacy Policy documents - I can easily find, read, and understand the privacy policy and/or terms of service.
    a. The company clearly discloses which Terms of Service (ToS) apply to the product/service in question.
    b. The ToS are easy to find.
    c. The company clearly discloses which Privacy Policy (PP) applies to the product/service in question.
    d. The PP is easy to find.
11. ToS & Privacy Policy change notification - The company provides clear notification when it changes its privacy policy and/or terms of service.
    a. Commitment to notify users about changes to the terms of service
    b. Maintains a public archive or change log of the terms of service
    c. Commitment to notify users about change to the privacy policy
    d. Maintains a public archive or change log of the privacy policy

Security

12. Encryption - Information I provide is encrypted so that it can't be easily read or used by attackers.
    a. All transmission of user communications is encrypted by default.
    b. All transmission of user communications is encrypted by a secure algorithm.
    c. Users can secure their content using end-to-end encryption.
    d. End-to-end encryption is enabled by default.
13. Known Exploit Resistance - The product is protected from known software vulnerabilities that present danger from attackers.
    a. The software is secure against known bugs and types of attacks.
    b. All known CVE or CWE should be fixed.
14. Authentication - A product has an authentication system that corresponds to the sensitivity of the user data it manages. And a product that has an authentication system resists attempts to break it.
    a. If a product supports user accounts, it has an authentication system for accessing those accounts.
    b. If the product uses a password/passphrase for authentication, it allows all reasonable characters as input.
    c. If the product uses a password/passphrase for authentication, it requires that passwords are at least 8 characters long.
    d. If the product uses a password/passphrase for authentication, the password/passphrase may be at least 20 characters long.
    e. If the product uses a password/passphrase for authentication, it requires that passwords are reasonably complex.
    f. If the product uses a password/passphrase for authentication, it is compatible with popular password managers.
    g. If a product is packaged with an account with default credentials, those credentials are unique to the instance of the product
    h. If a product has an authentication system, the user must authenticate each time they want to use the product

   i. If a product has an authentication system, it requires at least two pieces of information to authenticate users
   j. For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication.
   k. For products that handle sufficiently sensitive data, users can choose to use multi-factor authentication whenever the product is activated, or when a device is unrecognized.
   l. The product allows users to be notified via an out-of-band medium when account security settings are changed.
   m. To change a password/passphrase/pin, a user must enter the previous password/passphrase/pin, or have access to a secondary system that is used to reset it.
   n. The product notifies users when account security settings have changed.
   o. If the product has an authentication system, it also has a system to prevent brute-force/dictionary attacks
15. Security Oversight - The company is a responsible caretaker of my data.
   a. The company has systems in place to limit and monitor employee access to user information.
   b. The company has an internal security team that conducts security audits on the company's products and services.
   c. The company commissions third-party security audits on its products and services.
16. Security Over Time - The product is kept protected with software updates for a clearly defined and communicated period of time (i.e., the product life cycle).
   a. The product life cycle is communicated to the potential owner before purchase.
   b. Software updates are authenticated.
   c. Automatic software updates
   d. Notification of software updates
   e. Ease of installation of software updates
   f. The software can be kept up-to-date for security issues.
17. Vulnerability Disclosure Program - The company is willing and able to address reports of vulnerabilities.
   a. The company has a mechanism (ex: a bug bounty program) through which security researchers can submit vulnerabilities they discover.
   b. The company discloses the timeframe in which it will review reports of vulnerabilities.
   c. The company commits not to pursue legal action against security researchers.

Test Methodology

CR Privacy & Security Testing consists of three primary methodologies outlined below.

1. UI/UX Evaluation
    - Test the Password creation rules to determine the level of complexity required.
    - Test and look for requirements for additional user authentication options (Bio, MFA, PIN, and etc.)
    - Validate Firmware update options offered.
    - Validate Software update options offered.
    - CVE database known exploits lookup.
    - Review data control options in UI/UX.
2. Technical Test
    - Security features (Set up the device and note the privacy/security settings and features available to the user, such as cert pinning, root detection, backup option, stack protection, etc.)
    - Perform an extensive Brute-force dictionary attack.
    - Continuous network traffic capture, processing and analysis to validate that all data is encrypted in transmission.
    - Data encryption at rest (Local file system inspection). Validate that all data created or information stored locally on the host device is encrypted.
    - Perform Vulnerability scanner testing (i.e., light penetration testing).
    - Confirm if CVE database known exploits are fixed.
    - Detect third-party tracker's SDKs.
    - Analyze network traffic endpoints.
3. Document Review
    - CR reviews privacy policies, terms of service, EULA and other public, legally binding, documentation to determine what practices a company commits to in writing.