epiphan video

capture • stream • record

Security White Paper for the Pearl Family of video encoders

Document number: EPN110-2

Author: Epiphan Video

Publication Date: Jan 10, 2025

Revision History

Revision	Date	Revised By	Description
1	Jan 10, 2025	Y.Touray	Initial draft

Introduction 4

Epiphan security programme overview 4

Security by design 4

Security in testing 5

Organizational security 5

Employee Awareness and Training 5

Confidentiality and Data Protection 6

Incident Response 6

Feedback welcome 6

What is Epiphan Pearl 6

Technical description 7

Operating System 7

Table 1 Default incoming and outgoing ports 8

Network connectivity and security 9

Management interfaces 10

Securing Web user interface and REST API access 10

TLS 1.2 Supported Ciphers 11

Securing the Built-In Screen on Pearl Devices 11

Security best practises 12

Introduction

At Epiphan Video, we are committed to delivering secure, reliable, and high-performance products and services. The Epiphan Pearl line of video encoders, as standalone devices, are designed with robust security features to ensure the protection of sensitive information and seamless operation in diverse environments. This white paper outlines the security measures implemented in the Pearl video encoders, the development practices ensuring ongoing security, and the processes for addressing potential vulnerabilities.

The intention of this Security Whitepaper is to ensure that people and enterprises responsible for procurement, installation, maintenance, and operation of the Epiphan Pearl line of video encoders (Pearl-2, Pearl Nexus, Pearl Mini, and Pearl Nano), have relevant security-related information available to them in order to assist them with the secure installation and operation of their systems.

This security whitepaper describes the main technical aspects of Pearl-2, Pearl Nexus, Pearl Mini, and Pearl Nano systems that are relevant for IT security. It is intended mainly for systems integrators, administrators and other personnel that are responsible for procurement, installation, configuration, and maintenance of these devices.

Epiphan security programme overview

Epiphan Video takes the subject of security for all its products seriously, and it has developed sophisticated processes that are used throughout the design, testing, and manufacturing operations of the company, to ensure that appropriate levels of security are made available in its products that are supplied to customers. Epiphan Video has always prioritized the security of its products and developed robust, comprehensive processes to ensure that security is baked into every stage of the product lifecycle. From the initial design phase, through rigorous testing, and into the manufacturing operations, Epiphan remains committed to delivering products that meet the highest security standards. The company recognizes that the security landscape is constantly evolving, and therefore, it continually updates and refines its security protocols to address emerging threats and vulnerabilities. This proactive approach to security ensures that Epiphan products remain resilient and trustworthy for customers across all industries.

Security by design

Epiphan utilises a ‘security by design’ approach to hardware and software development, and strives to keep systems as free from vulnerabilities, and impervious to attacks as possible. This is achieved through proactive measures such as continuous testing, authentication safeguards, and adherence to best available programming practices. This methodology integrates security considerations into every phase of hardware and software development. This approach prioritizes the creation of systems that are inherently resistant to vulnerabilities and attacks.

To achieve this, Epiphan implements a multi-faceted strategy that includes rigorous and continuous testing to identify and address potential weaknesses before they can be exploited. Robust authentication safeguards are also employed to ensure that only authorized users can access sensitive data and systems. Additionally, Epiphan adheres to industry-recognized best practices in programming, incorporating established security principles and techniques into its development processes.

By adopting this comprehensive approach to security, Epiphan aims to minimize the risk of successful attacks and maintain the confidentiality, integrity, and availability of its systems and data.

Security in testing

The Epiphan Video Quality Assurance department incorporates security testing into its standard operating procedures. These processes aim to identify vulnerabilities in the Epiphan Pearl's security mechanisms, which are designed to protect data and maintain intended functionality.

To augment the robustness of our systems, we have integrated a rigorous firmware scanning protocol into our development cycle. Each firmware version, before being deployed, is subjected to meticulous scrutiny using a suite of sophisticated third-party penetration and vulnerability assessment tools. These tools generate comprehensive reports that are subsequently leveraged by our engineering team. This feedback loop enables us to proactively identify and rectify vulnerabilities, thereby continuously fortifying the security posture of the Epiphan Pearl and ensuring that our customers benefit from a product that is resilient against emerging threats.

Organizational security

Epiphan Video recognizes that robust organizational security is fundamental to safeguarding the integrity, confidentiality, and availability of its products, services, and the sensitive data entrusted to us by our valued customers. We have implemented a multi-layered approach to organizational security that encompasses policies, procedures, and technologies designed to mitigate risks and ensure business continuity.

Employee Awareness and Training

Our employees are our first line of defense against security threats. We provide comprehensive security awareness training to all staff members, educating them on the latest security best practices, potential risks, and their role in maintaining a secure environment. This training covers topics such as social engineering, phishing, password hygiene, data handling, and incident reporting.

Confidentiality and Data Protection

Epiphan Video handles sensitive customer and company data with the utmost care. All employees are required to sign confidentiality agreements that outline their responsibilities for protecting confidential information. We have implemented strict data protection policies and procedures that govern the collection, storage, processing, and transmission of data. Access to sensitive data is restricted to authorized personnel on a need-to-know basis.

Incident Response

In the event of a security incident, Epiphan Video has a well-defined incident response plan in place. This plan outlines the procedures for identifying, containing, and eradicating threats, as well as for communicating with affected parties and restoring normal operations. Our incident response team is trained and equipped to handle security incidents quickly and effectively.

Feedback welcome

Epiphan Video values and appreciates feedback from our customers. Your input is instrumental in helping us design and develop secure, award-winning video encoders that meet your needs and expectations.

Therefore, we encourage you to actively participate in our security enhancement efforts by reporting any vulnerabilities you may discover in our products.

To report a security vulnerability, please send an email to our dedicated security team at admins@epiphan.com. Our team of security experts is committed to promptly investigating and addressing all reported vulnerabilities to ensure the ongoing safety and reliability of our products.

What is Epiphan Pearl

Epiphan Video designs and manufactures high-performance video production hardware and cloud-based tools that are as versatile as they are accessible. As purpose-built appliances, Epiphan Pearls can capture, stream, and record broadcast-quality video while drawing on the cloud for more efficient production, management, and distribution.

Content creators and organizations around the world rely on the Epiphan ecosystem for a wide range of video applications, empowered by:

- Multistreaming technology: Powerful but easy-to-use streaming and recording capabilities to reach audiences wherever they are
- Cloud-based management: Remote access, configuration, and monitoring from anywhere with an Internet connection through the centralized Epiphan Cloud dashboard
- Flexible architecture: An open-platform approach that allows consumers and professionals to evolve their investment over time
- Productive partnerships: A growing network of innovative partners that enable new features and unlock efficiency
- Long-term reliability: Dependable performance and rock-solid customer support

Technical description

This document aims to comprehensively address the security considerations pertinent to all models of the Epiphan Pearl. The various models of Pearl share a significant number of features and core functionalities, this document will provide clear distinctions and highlight specific instances where certain security information applies exclusively to a particular model.

It is important to acknowledge that the Pearl's installation and configuration options are numerous and adaptable to diverse environments and use cases. This inherent flexibility allows for a high degree of customization during installation, enabling organizations to implement security measures that are tailored to their specific needs and risk profiles. The operating system, including the periodic firmware updates are installed as a read-only partition that cannot be modified after the installation process.

Operating System

The Epiphan Pearl's operating system is built on a foundation of a highly customized Linux distribution. This customization goes beyond mere configuration; it involves stripping down the operating system to its bare essentials, retaining only the libraries and packages that are directly necessary for the Epiphan Pearl's functionality. This minimalist approach significantly reduces the potential attack surface by eliminating unnecessary components that could be exploited by malicious actors.

Furthermore, all network ports and services that are not explicitly required for operation are disabled by default. This "closed by default" principle adds another layer of security by preventing unauthorized access and minimizing the risk of exposure to network-based threats.

The operating system, along with periodic firmware updates, is installed on a read-only partition. This read-only attribute ensures the integrity of the system by preventing any modifications after installation. This design choice effectively thwarts attempts to tamper with the operating system or introduce malicious code.

In addition to the read-only protection, the Epiphan Pearl enforces a strict separation between system data and user data, such as images and videos. This segregation of data further enhances security by preventing unauthorized access or modification of critical system files and settings.

The combination of these security measures – the customized Linux operating system, the closure of unnecessary network ports, the read-only system partition, and the separation of system and user data – creates a robust security framework that helps protect the Epiphan Pearl from a wide range of potential threats.

The following table lists the default incoming and outgoing network ports, transport protocol(s) used for each and a brief description of what each port is used for.

Table 1 Default incoming and outgoing ports

Port (or range)	Protocol	Default state	Direction	User configurable	Description
22	TCP	Enabled	Outbound	Yes	SSH for remote support by Epiphan technical support
80	TCP	Enabled	Inbound		Provides access to: ● Web interface ● API for third-part control ● Live video preview ● Switcher ● Epiphan Live
123	TCP UDP	Disabled	Inbound	Yes	If enabled, Pearl can be used as an NTP time server for local NTP clients
123	TCP UDP	Enabled	Outbound	Yes	Used by Pearl to synchronize its local time with network time servers
443	TCP	Disabled	Inbound	Yes	When enabled, this port provides secure HTTPS access to: ● Web interface ● API for third-party control ● Live video preview ● Switcher

					• Epiphan Live
443	TCP	Enabled	Outbound	Yes	Required for: • Epiphan Edge • Periodic firmware check • Firmware download
554 to 554+(x-1)	TCP UDP	Enabled	Inbound	Yes	RTSP streaming of a Pearl channel. Number of ports used depends on number of channels on Pearl
32768 - 61000	UDP	Enabled	Outbound	Yes	Stream video and audio to RTSP client after a successful RTSP connection
5353	UDP	Enabled	Inbound	Yes	Multicast DNS to easily discover the hostname of the Pearl on a local area network without the need for a central DNS server
8000 to 8000+(x-1)	TCP	Enabled	Inbound	Yes	Flash (FLV) live stream and MPEG-TS streaming on your network

Network connectivity and security

The Epiphan Pearl's built-in 10/100/1000 Mbps Ethernet interface offers network connectivity, with an option for a secondary interface via USB-to-Ethernet adapter on Pearl-2, Pearl Mini, and Pearl Nexus models (firmware 4.24.0 and later).

Routing between the two network interfaces, when both are connected, is not supported.

With network support, IEEE 802.1x authentication and authorization can be implemented using mutual authentication to prevent unauthorized network access. Supported Extensible Authentication Protocols (EAP) include PEAP (username and password), EAP-TTLS (username and password or digital certificate), and EAP-TLS (digital certificate).

Management interfaces

Epiphan Pearl devices provide a variety of interfaces to manage, control, and configure their settings. These interfaces include:

- Web-based GUIs,
- REST APIs,
- Built-in screen

Each interface can be individually configured with security measures to restrict access and prevent unauthorized changes.

Securing Web user interface and REST API access

Epiphan Pearl's web-based Graphical User Interface (GUI) requires users to log in with a username and password. A Role Based Access Control (RBAC) model manages access to system features, ensuring that users only have the permissions required for their role.

Three roles have been defined:

- Administrator: This role possesses the highest level of system privileges. Administrators are responsible for the overall configuration and management of the system, including user account management, system settings, and can also perform day-to-day tasks as well.
- Operator: Operators interact with the system to perform day-to-day tasks and operations. Their access is restricted to operational functions as defined by the system administrator.
- Viewer: Viewers have read-only access to the system. They can monitor system status and view data, but cannot make any changes to the system configuration or settings.

To further enhance security, the Pearl Security system offers flexibility in user authentication. Users can either be authenticated against the device's internal database or an external LDAP (Lightweight Directory Access Protocol) server. This allows for seamless integration with existing enterprise user management systems and centralized authentication.

Additionally, HTTPS can be enabled to further enhance security by making sure that all data transfer between a web browser or a third-party application using the Pearl REST API and the Epiphan Pearl is encrypted while in transit. When this is enabled, the Pearl device exclusively utilizes TLS version 1.2 to secure the data in transit.

To prevent potential vulnerabilities, previous versions of the TLS protocol are deactivated and cannot be used in negotiations.

TLS 1.2 Supported Ciphers

The Pearl's TLS 1.2 implementation supports a range of ciphers, detailed in the table below. These ciphers are selected to balance strong encryption with performance and compatibility across different systems.

Table 2 Supported TLS ciphers

Name	Auth	Encryption	Key exchange	MAC
ECDHE-RSAAES128-SHA256	RSA	AES(128)	ECDH	SHA256
ECDHE-RSAAES256-SHA384	RSA	AES(256)	ECDH	SHA384
ECDHE-RSAAES128-GCMSHA256	RSA	AESGCM(128)	ECDH	AEAD
ECDHE-RSAAES256-GCMSHA384	RSA	AESGCM(256)	ECDH	AEAD
ECDHE-RSACHACHA20-POLY1305	RSA	CHACHA20/ POLY1305(256)	ECDH	AEAD

Securing the Built-In Screen on Pearl Devices

There are several methods to enhance security and control access to the integrated screen on models of Pearl with built-in screens, including the Pearl-2, Pearl Mini, and Pearl Nano. These security measures offer different levels of protection and can be tailored to specific needs and preferences.

1. PIN Protection

Implementing a PIN (Personal Identification Number) requirement adds a layer of security by demanding a code to unlock and access the screen's content and functionality. This prevents unauthorized users from viewing or interacting with the device.

2. Restricting Screen Functionality

Limiting the screen to "read-only" or "view-only" mode restricts user interaction, allowing content to be viewed but not modified. This is useful in scenarios where information should be displayed but not altered, such as in public kiosks or information displays.

3. Automatic Screen Timeout

Configuring the screen to turn off automatically after a specified period of inactivity conserves power and enhances security. By automatically shutting down when not in use, it reduces the risk of unauthorized access and data exposure.

4. Disabling the Screen

Completely disabling the screen prevents any content from being displayed and eliminates all screen-based interaction. This option provides maximum security when screen functionality is not required.

Security best practises

Epiphan places a high premium on security and has integrated robust security measures throughout all stages of product development, including design, testing, and manufacturing. These stringent processes ensure that customers can access appropriate levels of security when using Epiphan video encoders.

To further enhance the security of your system when using Epiphan video encoders, Epiphan strongly recommends adhering to the following best practices:

- Strong Passwords: During the initial device setup, it is crucial to set strong and unique passwords for all user roles, including administrator, operator, and viewer. Strong passwords typically include a combination of uppercase and lowercase letters, numbers, and special characters.
- HTTPS: Enable HTTPS for all device management tasks. HTTPS encrypts data transmitted between your web browser and the device, protecting sensitive information from interception.
- Secure Streaming Protocols: Whenever possible, utilize secure live streaming protocols such as RTMPS, HLS over HTTPS and SRT (Secure Reliable Transport). These protocols encrypt your video streams, preventing unauthorized access and ensuring content integrity.
- Secure File Transfers: When transferring files from your Pearl device to network-attached storage, employ secure file transfer protocols like AWS S3 (Amazon Web Services Simple Storage Service), SFTP (SSH File Transfer Protocol), SCP (Secure Copy Protocol), or CIFS (Common Internet File System). These protocols encrypt your data during transfer, safeguarding it from unauthorized access.
- Feature Management: Deactivate any features that are not required for your specific workflow. This minimizes the potential attack surface and reduces the risk of unauthorized access.
- Physical Security: Install your Epiphan device in a secure location with restricted access. This helps prevent physical tampering and unauthorized use.
- Firmware Updates: Regularly check for and install firmware updates for your Pearl device as they become available. Firmware updates often include security patches that address known vulnerabilities and enhance overall system security.

By implementing these recommended best practices and taking advantage of the built-in security features of Epiphan video encoders, organizations can achieve the level of security that aligns with their specific requirements and risk tolerance. Remember that security is an ongoing process, and it's essential to stay informed about emerging threats and adapt your security measures accordingly.