Barco | Whitepaper

ClickShare Security Advisory

DATE 17/12/2019

LIMITED DISTRIBUTION – FOR CLICKSHARE CUSTOMERS AND RESELLERS

AUTHOR David Martens

Table of content

Introduction

Cybersecurity is a continuous topic and can pose a threat throughout the lifecycle of any product. Barco ClickShare products are designed with safety, privacy, and confidentiality in mind. To keep our solutions at minimum vulnerability, we implement necessary fixes and advanced features with every quarterly release. Next to being ISO27001 certified, Barco also has a Product Security Incident Response Team (PSIRT) that continuously monitors privacy and security risks and drives security improvements to ensure ClickShare maintains its earned reputation as one of the most trusted wireless collaboration tools in the market.

The newest December update v1.9.1.7 for CS-100 (Huddle), CSE-200, CSE-200+ and CSE-800 addresses a set of exposures that have been discovered through ethical hacking. We patched all vulnerabilities that gave direct opportunity to tamper with the devices or get access to confidential information. Others are planned to be patched in the March release of 2020, these are additional security measures, which add an additional layer of security to implement defense in depth. For the CS-100 and CSE-200 the hardware vulnerability in the i.MX6 SoC cannot be patched and therefore, people with bad intent who have physical access to the box can open the Base Unit and via hardware tampering change the device to receive maliciously crafted firmware images.

Although we haven't received any reports of vulnerabilities being exploited in the wild, we strongly recommend updating your ClickShare systems, both Base Unit and Button.

Discovered vulnerabilities

Button

Public Identifier	**CVE-2017-7932**
Risk	A secure boot vulnerability has been identified in the High Assurance Boot (HAB) of the i.MX 283 SoC during the parsing of a certificate in a security enabled configuration. Specific functions are used to process a certificate from its native form. Under certain conditions, it is possible to bypass the signature verification by using a specially crafted certificate.
Prerequisites	The attacker must have access to the firmware encryption key in the SoC to be able to encrypt the forged content, can only be done via JTAG (CVE-2019-18827) or command line access (CVE-2019-18830).
Impact	This vulnerability could lead to the execution of an unsigned and unauthorized image on the target, given that also the prerequisites are fulfilled.
Patched	No, this is a vulnerability in the ROM code of the chipset, which cannot be

	changed.

Public Identifier	**CVE-2019-18827**
Risk	On the ClickShare Button (R9861500D01) the JTAG debug interface of the i.MX 28 SoC is only disabled in software at initial stage of the bootloader and not permanently disabled. The official documentation provided by NXP, the SoC manufacturer, does not specify any way of disabling the JTAG access permanently for production devices. This means that JTAG access is possible when the system is running code from ROM before handing control over to user software.
Prerequisites	Physical access to the Button and opening the Button to access the PCBA are necessary.
Impact	This vulnerability could give the attacker access to the one-time programmable (OTP) AES encryption key in the i.MX28 SoC, which is used for decryption of software images during boot. The key is not readable but can be used to encrypt the forged content.
Patched	Yes, NXP provided us with internal documentation that allowed Barco to close the JTAG interface permanently after installation of the 1.9.1 firmware.

Public Identifier	**CVE-2019-18832**
Risk	The i.MX28 SoC used in the Button provides a way to provision a one-time programmable (OTP) AES encryption key to be used for multiple purposes, one of which is the decryption of software images during boot.
Prerequisites	The attacker must have access to the firmware encryption key in the SoC to be able to encrypt the forged content, this can only be done via JTAG (CVE-2019-18827) or command line access (CVE-2019-18830).

Impact	An attacker which can use the OTP key is able to forge arbitrary firmware images which will be accepted as bootable on all Buttons.
Patched	No, having the same firmware encryption key on all Buttons is a design choice to provide the same firmware images to all Buttons

Public Identifier	**CVE-2019-18830**
Risk	The program "dongle_bridge", controlling USB functionality on the Button, is responsible for the implementation of multiple commands used by the USB host to control the Button behaviour. The program contains multiple OS command injections due to unsafe use of the system() C runtime library function, where user provided input is used to build a command line without any prior validation or sanitisation.
Prerequisites	Physical access to the Button and connect it via USB to your laptop.
Impact	An attacker, able to send commands to the Button, is able to inject and execute arbitrary OS commands with the privileges of the dongle bridge process, in this case running as the nobody user (low level privileges).
Patched	Yes, the OS command injections have been removed.

Public Identifier	**CVE-2019-18831**
Risk	The communication between a Button and a Base Unit happens via a mutually authenticated TLS connection. A test device certificate was discovered on the Button, together with the corresponding private key. These credentials are signed by the production root certificate authority.
Prerequisites	Physical access to the Button and connect it via USB to your laptop. Access to the running OS on the Button can then be obtained via the OS command injection vulnerability (CVE-2019-18830).

Impact	An attacker able to gain access to a software image running on the Button may obtain credentials used to authenticate to arbitrary devices.
Patched	Yes, test device certificate and corresponding private key have been removed from the Button filesystem. Measures have been put in place in the development process to ensure that similar cases do not occur.

Public Identifier	**CVE-2019-18826**
Risk	The communication between a Button and a Base Unit happens via a mutually authenticated TLS connection, in order to protect privileged functionality such as changing device configuration or updating software components. The verification process is not correctly implemented and allows to use certificates which are not signed by the production root certificate authority.
Prerequisites	Physical access to the Button and connect it via USB to your laptop.
Impact	An attacker can use self-signed certificates to authenticate against the device, gaining access to otherwise restricted commands to change device configuration or push new firmware.
Patched	Yes, the verification process has now been correctly implemented and check for the signature of the root certificate authority.

Public Identifier	**CVE-2019-18824**
Risk	The content of the USB mass storage file system image, presented to the laptop connected via USB, is not validated before being used. Specifically, the mass storage file system image can be manipulated arbitrarily without being detected by the system.
Prerequisites	Physical access to the Button and connect it via USB to your laptop.

Impact	An attacker may manipulate the file system, placing crafted data which will be presented to any user plugging the device via USB. This can be exploited to e.g. plant malware on the Button.
Patched	Closing OS command injection (CVE-2019-18830), closing JTAG permanently (CVE-2019-18827), removing the test certificate (CVE-2019-18831) and correctly verifying the mutual TLS authentication (CVE-2019-18826) do close all known vulnerabilities which would allow attackers to forge the Button firmware image and push it onto the Button. The patch of this vulnerability is a verification step before the mass storage is presented to the laptop and is a second layer of defense. This is planned for the next release (end of March 2020).

Public Identifier	**CVE-2019-18828**
Risk	The root account for administrative access to the Linux operating system on the Button was found to have a weak, guessable password.
Prerequisites	Physical access to the Button and connect it via USB to your laptop and exploit the OS commandline injections (CVE-2019-18830) or open the Button and solder serial connector to the serial output pins.
Impact	An attacker with physical access is able to gain access to the system and obtain administrative rights, taking full control over the execution environment.
Patched	Yes. The password has been changed with seriously increased entropy (a combination of 26 symbols, numbers and characters) and the hashing algorithm has also been updated to the latest recommended standard (SHA-512)

ClickShare application

Public Identifier	**CVE-2019-18829**
Risk	Windows 7/8/8.1/10 automatically installs a driver and service for the ClickShare Button. The purpose of this is to improve the user experience by automatically launching the Clickshare_For_Windows.exe binary present on the Button. The

	functionality verifies that the binary is signed by Barco, so any modification of the main executable will prevent automatic execution. This binary will however load a number of DLL files based on the standard DLL search order, allowing for a zero-interaction compromise.
Prerequisites	Physical access to the Button and connect it via USB to your laptop.
Impact	An attacker, capable of modifying the USB mass storage content presented by the Button to the host system, is able to plant arbitrary code which will be side-loaded into the ClickShare application on start, while preserving the signature of the client binary stays intact.
Patched	Closing OS command injection (CVE-2019-18830), closing JTAG permanently (CVE-2019-18827), removing the test certificate (CVE-2019-18831) and correctly verifying the mutual TLS authentication (CVE-2019-18826) do close all known vulnerabilities which would allow attackers to forge the Button firmware image and push it onto the Button. The patch of this vulnerability is preventing that any DLL provided on the USB mass storage is loaded by the ClickShare application. This is planned for the next release (end of March 2020).

Public Identifier	**CVE-2019-18833**
Risk	The ClickShare application makes use of two communication channels, one for control and one for media backhaul. Both channels are encrypted: the control channel uses TLS, while the media channel uses symmetric encryption based on the Salsa20 cipher. It was found that the encryption key used to protect data passed through the media channel can be easily disclosed by conducting a Man-in-the-Middle attack against the Button's TCP connections towards the Base Unit. The key itself was found to be passed unprotected in the intercepted TLS communication.
Prerequisites	The attacker has to be in the vicinity of the Button and Base Unit to interfere with the Wi-Fi signals to execute a Man-in-the-Middle attack and he has to be in the possession of a valid ClickShare X.509 device certificate (signed by the production root certificate authority) and corresponding private key. This is made possible via the test device certificate and corresponding private key, which was found on the Button (CVE-2019-18831).

Impact	An attacker capable to execute a successful Man-in-the-Middle attack will be able to discover the agreed Salsa20 key in the intercepted TLS communication and use it to decrypt the media stream transferred from Button to Base Unit.
Patched	Yes, the test device certificate and corresponding private key have been removed from the Button (CVE-2019-18831). If by any means a Button or Base Unit device certificate is compromised, a blacklisting mechanism allows us to block certificates from our next release onwards. This blacklist mechanism is an additional security control to prevent that any compromised device certificate and corresponding private key can be abused to intercept shared media streams.

Base Unit (CS-100/CSE-200)

Public Identifier	**CVE-2017-7932 & CVE-2017-7936**
Risk	The i.MX6 SoC on the CS-100 and CSE-200 is known to be affected by two previously disclosed vulnerabilities pertaining to the High Assurance Boot functionality, which guarantees that only trusted code can be executed. One of the two is similar as the one reported on the i.MX28 SoC on the Button.
Prerequisites	The attacker must have physical access to the Base Unit, open the box and short circuit certain pins at boot time to be able to upload a special, correctly crafted firmware image to the Base Unit.
Impact	An attacker can bypass the High Assurance Boot security feature and subsequently compromise the Base Unit by executing arbitrary, untrusted code. This issue can also be exploited in a persistent manner by writing a crafted image to the eMMC storage.
Patched	No, this is a vulnerability in the ROM code of the chipset, which cannot be changed.

Public Identifier	**CVE-2019-18825**

Risk	File system encryption keys and firmware image encryption keys are shared across device families.
Prerequisites	The attacker must have physical access to the Base Unit, open the box and desolder the eMMC flash to extract the content and use that knowledge to get access to the shared keys.
Impact	An attacker who successfully compromised one Base Unit gains the ability to decrypt as well as produce valid encrypted images for any Base Unit based on the same SoC. This can be exploited to e.g. directly overwrite non-volatile memory contents such as the fallback partition with crafted images, based on vulnerability CVE-2017-7932 & CVE-2017-7936.
Patched	No, having the same filesystem and firmware encryption keys on all devices based on the same SoC is a design choice to increase the update speed and provide the same firmware images to all those devices.

Conclusion

All software vulnerabilities that can be considered as an entry point into the system have been patched in the 1.9.1.7 software update. Other, secondary, vulnerabilities will be patched in subsequent updates. The hardware vulnerabilities remain but can not be exploited without the required skillset, knowledge and time to alter the electronics on the ClickShare system. In addition, new entry points into the software system would have to be found to enter and modify the ClickShare system.

Recommendations

Keep your Base Units and Buttons up to date

Barco keeps improving ClickShare, this means extending existing features and adding new ones, but also providing security patches. Therefore, it is strongly recommended to keep the Base Units up to date with the latest available firmware, and ensure Buttons are updated. Updating ClickShare to the latest firmware can be done in 3 easy ways. More info on https://www.barco.com/en/clickshare/firmware-update

Buttons can be updated in two different ways:

- Buttons are updated over Wi-Fi when they are connected to a laptop for sharing. However, this is only done when they are connected to a host for a sufficient amount of time, approximately 10 to 15 minutes.
- Buttons can be connected via USB to the Base Unit, this is called “pairing”. Different configuration settings are then transferred to the Button and also new firmware is pushed

if applicable during the pairing process.

To ensure an update of all Buttons, Barco strongly recommends pairing all Buttons with the corresponding Base Unit immediately after the Base Unit has been successfully upgraded.

Manage Base Units through XMS (Cloud) management Platform to receive updates

XMS is Barco's secure cloud-based solution for the configuration, remote management and real-time status monitoring of your ClickShare and wePresent devices, distributed over different locations. Enjoy easy & automated (scheduling of) software updates, Base Unit configuration, creation of templates, remote wallpaper installation, user management and insights to drive Digital Workplace.

Keep Base Units locked away

In case you expect physical tampering of the hardware by malicious people Barco recommends keeping the Base Units locked away.

Change the default Wi-Fi password

Barco strongly recommends changing the default Wi-Fi password (only applicable when WPA2-PSK mode is used), this makes it again one step more difficult for malicious people, without physical access to your devices, to intercept the traffic between Button and Base Unit.

Change the default webUI password

Barco strongly recommends changing the default webUI password. Anyone with malicious intentions who can access the Base Unit locally or via adjacent networks will definitely verify if the Base Unit's webUI can be accessed to extract valuable information like e.g. Wi-Fi credentials.