Mesures de cybersécurité pour les caméras FireCatcher

Introduction

Araani NV veille à appliquer les meilleures pratiques en matière de cybersécurité lors de la conception, du développement et des tests des logiciels et du matériel afin de réduire au minimum le risque de failles qui pourraient être exploitées dans le cadre d'une cyberattaque.

La FireCatcher Camera a été testée et certifiée par l'association française CNPP pour la protection de la cybersécurité selon la norme ST LPMES – DEC 17-04 A – 11/02/2019 « Méthode d'évaluation de la robustesse des équipements de sécurité » avec un score de 2 sur 3. C'est le score le plus élevé qui peut être obtenu pour un objet de niveau composant tel que FireCatcher Camera.

Il est primordial de maintenir vos appareils à jour avec les derniers firmwares et logiciels approuvés qui incluent les dernières précautions en matière de cybersécurité. La souscription d'un contrat de service avec votre partenaire certifié Araani vous garantit un fonctionnement fluide et sécurisé pendant toute la durée de vie de FireCatcher Camera.

Vous trouverez ci-dessous une description des mesures qui ont été prises sur notre produit FireCatcher Camera pour assurer la cybersécurité.

Avis de non-responsabilité

La sécurisation d'un système consiste à protéger l'environnement complet et tous les périphériques. Cet environnement doit être optimisé dans son ensemble par un spécialiste en informatique connaissant parfaitement vos systèmes.

Contrôle d'accès basé sur les rôles

L'accès à FireCatcher Camera n'est possible que par l'utilisation de profils d'utilisateurs prédéfinis bénéficiant d'autorisations spécifiques.

Les mots de passe des rôles d'administrateur et d'opérateur sont uniques pour chaque lot de production et sont indiqués sur une étiquette amovible sur le produit, ainsi que dans le livret du guide d'installation rapide inclus. Veillez à retirer l'étiquette d'identification de la caméra avant de la fixer puis à retirer et conserver le livret du guide d'installation rapide de l'emballage.

Il faut savoir que vos FireCatcher Camera peuvent provenir de différents lots de production, ainsi elles ne possèdent donc pas nécessairement le même mot de passe.

Il est conseillé de modifier les mots de passe par défaut au moment de l'installation.

Araani NV ; Luipaardstraat 12 ; 8500 Kortrijk (Belgique) ; info@araani.com ; http://www.araani.com ; +32 (0) 56 49 93 94

Protocoles de réseaux

La FireCatcher Camera prend en charge divers moyens d'accéder à l'appareil sur le réseau pour la configuration, la maintenance, la gestion et l'intégration. Les services et les ports IP qui ne contribuent pas au fonctionnement de la FireCatcher Camera ont été désactivés et clôturés dans la mesure du possible.

Protocole	Port IP/TCP	Utilisation	FireCatcher Camera
http	80	Accès à l'interface web protocoles de communication basés sur http VAPIX, une interface de programme d'application AXIS ONVIF	Désactivé, utilisation de https uniquement.
https	443	Identique au http mais sécurisé	ACTIVÉ Les anciens protocoles d'authentification TLSv1.0 et TLSv1.1 sont désactivés par défaut.
RTSP	554	Diffusion vidéo	ACTIVÉ La visualisation anonyme est désactivée.
RTP	éphémère	Diffusion vidéo	ACTIVÉ
UPnP	49152	Protocole de découverte des dispositifs	DÉSACTIVÉ *
Bonjour	5353	Protocole de découverte des dispositifs, utilisé par l'outil Axis IP Utility.	ACTIVÉ Il est conseillé de le désactiver après l'installation initiale. *
SSDP	1900	Protocole de découverte des dispositifs (UPnP)	DÉSACTIVÉ *
WS-discovery	3702	Découverte des dispositifs (ONVIF)	ACTIVÉ Il est conseillé de le désactiver après l'installation initiale. *
Protocole Araani	5554, 5555	Protocole propriétaire Araani pour la communication des états et des alarmes dans le but d'une intégration VMS personnalisée.	Activé uniquement lorsque la licence est explicitement accordée.
NTP	1023	Port client pour la synchronisation horaire du réseau.	Client uniquement, utilisé uniquement lorsque NTP est configuré.
FTP	21	Transfert de fichiers	Désactivé par défaut sur Axis.
SSH	22	Accès à distance par Secure Shell	Désactivé par défaut sur Axis.
SNMP	161,162	Notification par e-mail	Désactivé par défaut sur Axis.
RTSPS	322	Diffusion sécurisée de vidéos	Désactivé par défaut sur Axis.
MQTT	1883	Communication entre dispositifs	Désactivé par défaut sur Axis.

Les protocoles discovery peuvent être désactivés dans la configuration FireCatcher Camera :

- Network Bonjour, Network UPnP et Network ZeroConf peuvent être activés/désactivés sous Settings (Paramètres) > Plain config (Configuration générale) > Network (Réseau).
- Webservice Discovery peut être activé/désactivé sous System (Système) > Plain config (Configuration générale) > WebService

Araani NV ; Luipaardstraat 12 ; 8500 Kortrijk (Belgique) ; info@araani.com ; http://www.araani.com ; +32 (0) 56 49 93 94

Diffusion vidéo limitée

Pour se protéger d'une attaque par déni de service (DoS) provoquant une saturation des demandes de diffusion vidéo, le nombre de clients vidéo a été limité à 5.

Ceci est configuré sous System (Système) > Plain config (Configuration générale) > Image > Max viewers (Nombre maximal de visionneurs).

La connexion à un flux vidéo requiert des informations d'identification. Un profil de spectateur a été créé pour prendre en charge l'accès authentifié à la diffusion vidéo.

Logiciel signé

Le logiciel de la FireCatcher Camera est distribué sous forme de paquet ACAP signé uniquement. La vérification de la signature est effectuée pendant l'installation de l'application ACAP. Cela garantit que l'ACAP est authentique et qu'aucun code n'a été injecté ou falsifié. L'utilisation des ACAP signés sera bientôt rendue obligatoire par Axis.

Configuration de la date et de l'heure

En matière de sécurité, il est important que la date et l'heure soient correctes. Il est recommandé de synchroniser l'horloge de la FireCatcher Camera avec un serveur NTP (Network Time Protocol). Dans tous les cas, l'heure et la date doivent être vérifiées et réglées si nécessaire à chaque maintenance.

Autre

Araani met à disposition un fichier de configuration prédéfini qui contient tous les paramètres conseillés et peut être utilisé pour configurer (ou reconfigurer) les paramètres de cybersécurité de la FireCatcher Camera, en utilisant Axis device manager.

Pour plus d'informations sur le renforcement des caméras Axis, rendez-vous sur https://help.axis.com/axis-os-hardening-guide.

Araani NV ; Luipaardstraat 12 ; 8500 Kortrijk (Belgique) ; info@araani.com ; http://www.araani.com ; +32 (0) 56 49 93 94