CYBERSÉCURITÉ

Gestion du cycle de vie des dispositifs

Les risques de cybersécurité sont présents à chaque étape du cycle de vie d'un dispositif en réseau, de sa production à son retrait d'exploitation. Si ces risques sont négligés, ils peuvent occasionner des perturbations opérationnelles et une perte de la confidentialité, de l'intégrité et de la disponibilité des données. Par conséquent, tous les acteurs, du fournisseur au client final, doivent s'approprier la gestion des risques.

Dans le processus d'approvisionnement, la prise en compte de la sécurité tout au long du cycle de vie des dispositifs est donc déterminante. Un fabricant doit appliquer des mesures pour atténuer les risques de cybersécurité avant que son produit parvienne au client, pendant que le produit est en service et lorsque le produit est mis hors service.

Les pages suivantes dressent un tour d'horizon des technologies, des outils, des bonnes pratiques et des méthodes et processus qu'Axis a mis en place pour réduire les risques tout au long du cycle de vie d'un dispositif Axis.

Base de la sécurité : Axis Edge Vault, AXIS OS, Modèle de développement de sécurité Axis

PRODUCTION

DISTRIBUTION

MISE EN ŒUVRE

EN SERVICE

MISE HORS SERVICE

Base de la sécurité : matériels, logiciels et méthode

Protection de l'intégrité des produits et réduction du risque de vulnérabilités dès le départ

Plateforme de cybersécurité Axis Edge Vault
Cette plateforme matérielle prend en charge des fonctions qui protègent l'identité et l'intégrité du dispositif contre les accès non autorisés. Vous pouvez ainsi démarrer le dispositif en toute sécurité et l'intégrer, en étant assuré que les données sensibles telles que les clés sont protégées.

Système d'exploitation AXIS OS
AXIS OS pilote toute une série de dispositifs Axis. Incorporant les bonnes pratiques du secteur en matière de gestion des vulnérabilités, AXIS OS fournit la plateforme pour déployer des fonctions et correctifs de sécurité logicielle de manière rapide et efficace sur un grand nombre de produits.

Modèle de développement de sécurité Axis (ASDM)
Cette méthodologie appliquée chez Axis consiste à réduire le risque de commercialiser des produits contenant des vulnérabilités logicielles. Le modèle ASDM veille à inscrire les considérations de sécurité au cœur du développement logiciel. Entre autres, il mobilise des analyses de risques, la modélisation des menaces, l'analyse du code, des tests de pénétration, un programme de chasse aux bugs, la recherche de vulnérabilités et leur gestion.

Transparence
L'instauration de la confiance compte pour une part importante de la méthode de travail d'Axis. En tant qu'autorité de numérotation CVE (Common Vulnerability and Exposures), Axis publie des informations sur les vulnérabilités et en avise les acteurs concernés pour que les clients puissent prendre les mesures appropriées. Nous publions également la liste des ingrédients logiciels (SBOM, Software Bill Of Materials) d'AXIS OS.

PRODUCTION ET DISTRIBUTION

Atténuation du risque de compromission de composants

- **Chaîne d'approvisionnement :** Les composants critiques sont fournis directement par des fournisseurs stratégiques. Axis collabore étroitement avec ses partenaires de fabrication. Les procédés de production sont contrôlés et les données partagées avec Axis 24h/7j, permettant ainsi des analyses en temps réel et une transparence totale.
- **Axis Edge Vault :** Installé sur les dispositifs Axis pendant la production, Axis Edge Vault englobe les fonctions suivantes :
  - **Magasin de clés sécurisé,** qui fait appel à des modules de calcul cryptographique (élément sécurisé, module TPM, environnement d'exécution de confiance [TEE], ...) pour le stockage sécurisé des clés.
  - **Signature de firmware,** qui garantit l'authenticité du système d'exploitation AXIS OS. Cette fonction vérifie qu'un nouveau firmware à télécharger et à installer sur le dispositif est également signé par Axis.
  - **Amorçage sécurisé,** qui permet au dispositif de vérifier que le firmware possède une signature Axis. Si le firmware n'est pas autorisé ou a été modifié, le processus d'amorçage est interrompu et le dispositif cesse de fonctionner. Ensemble, la signature de firmware, l'amorçage sécurisé et la remise aux paramètres d'usine du dispositif offrent une protection contre les modifications malveillantes pendant le transport du dispositif.
  - **ID de dispositif Axis,** qui est un certificat unique avec les clés correspondantes, prouvant l'authenticité d'un dispositif Axis. Basé sur la norme IEEE 802.1AR, l'ID de dispositif Axis permet l'identification sécurisée du dispositif et son intégration à un réseau.
  - **Système de fichiers chiffré**, qui protège la configuration et les informations spécifiques au client stockées qu'il contient contre l'extraction ou la falsification quand le dispositif est inutilisé, par exemple pendant son transport entre un intégrateur systèmes et le client final.

MISE EN ŒUVRE

Prise en compte des risques d'introduction de produits compromis ou insuffisamment protégés sur le réseau, points d'entrée potentiels pour des accès non autorisés, l'extraction de données sensibles et le transfert de données falsifiées entre terminaux du réseau

- **Remise aux paramètres d'usine :** Effectuez une remise aux paramètres d'usine sur le dispositif avant de le configurer. Cette précaution garantit que le dispositif est totalement exempt de logiciels et de configurations indésirables, puisque le seul logiciel restant est AXIS OS et ses paramètres par défaut.
- **Recherche du firmware le plus récent pour le dispositif :** Il est possible qu'un certain temps s'écoule entre la production et la mise en œuvre du dispositif. Il est donc judicieux de rechercher sur le site web Axis le firmware le plus récent, qui peut contenir les tout derniers correctifs du dispositif en question.
- **ID de dispositif Axis :** Pour que le réseau accueille exclusivement des dispositifs Axis authentiques, il est possible de vérifier l'ID de dispositif Axis, soit par authentification IEEE 802.1X, soit en établissant une connexion réseau sécurisée par le protocole HTTPS. Sur un réseau IEEE 802.1X, l'ID de dispositif Axis peut servir à renforcer la sécurité et à raccourcir les délais de déploiement.
- **Magasin de clés sécurisé :** Mobilisant des modules de calcul cryptographique, le magasin de clés sécurisé conserve les informations sensibles (par ex. ID de dispositif Axis, clés chargées par le client...) et empêche les accès non autorisés ou l'extraction malveillante d'informations sensibles, même en cas de compromission du dispositif.
- **Système de fichiers chiffré :** Cet environnement garantit qu'aucune donnée stockée dans le système de fichiers ne peut être extraite ou falsifiée lorsque le dispositif est inutilisé.
- **Guides de renforcement de la sécurité :** Le guide de protection d'AXIS OS (AXIS OS Hardening Guide), disponible sur le portail AXIS OS du site web Axis, définit une configuration de référence pour se prémunir des menaces courantes, en proposant des bonnes pratiques et des conseils techniques. Des guides de protection sont également proposés pour le logiciel de gestion vidéo AXIS Camera Station et les switchs réseau Axis.
- **Guide d'analyse de sécurité AXIS OS :** Axis recommande d'exécuter des analyses de sécurité sur les dispositifs Axis pour vérifier s'ils comportent des vulnérabilités ou des configurations peu sûres. Le guide d'analyse de sécurité AXIS OS (AXIS OS Security Scanner Guide) fournit des recommandations pour résoudre certaines remarques des analyseurs et recense les « faux positifs » courants.
- **AXIS Device Manager :** Cet outil simplifie la configuration et la gestion locales des dispositifs Axis. Il permet de traiter de manière globale les tâches d'installation et de sécurité, comme la gestion des identifiants des dispositifs, le déploiement des certificats, la désactivation des services inutilisés et la mise à niveau d'AXIS OS.

PRODUCTION

DISTRIBUTION

MISE EN ŒUVRE

EN SERVICE

MISE HORS SERVICE

EN SERVICE

Prise en compte des risques en lien avec l'exécution de firmwares comportant des vulnérabilités connues, la mise à jour de dispositifs avec un firmware non authentifié ou l'expiration de configurations sécurisées

> **Mise à niveau du firmware :** Il est impératif de préserver la cybersécurité d'un dispositif Axis en maintenant son firmware à jour, soit par la voie active AXIS OS, soit par la voie de support à long terme LTS (Long-Term Support). Les mises à jour de firmware sont gratuites et contiennent des correctifs de sécurité, quelle que soit la voie choisie. La fonction de signature de firmware garantit que seuls des firmwares Axis authentiques peuvent être installés.

> **AXIS Device Manager Extend :** Cet outil, qui complète AXIS Device Manager, permet de gérer à distance les dispositifs Axis et simplifie l'extension des tâches de maintenance comme la mise à jour du firmware d'un dispositif.

> **Gestion des vulnérabilités :** Axis propose un service de notifications de sécurité, auquel vous pouvez vous abonner pour obtenir des informations sur les vulnérabilités et d'autres thèmes liés à la sécurité.

> **Guide d'analyse des incidents AXIS OS :** Le guide AXIS OS Forensic Guide propose des conseils techniques à l'intention des personnes chargées de l'analyse post-incident des dispositifs Axis, en cas de cyberattaque sur le réseau environnant et l'infrastructure informatique où est installé un dispositif Axis.

> **Signature de vidéo :** Lorsque cette fonction est activée sur une caméra compatible, des signatures cryptographiques sont ajoutées au flux vidéo avant qu'il quitte la caméra, permettant ainsi aux opérateurs de vérifier si la vidéo a été falsifiée. Cette fonction est particulièrement importante dans le cadre d'une enquête ou de poursuites judiciaires.

MISE HORS SERVICE

Prise en compte des risques pour les dispositifs en fin de support qui comportent des vulnérabilités connues non corrigées, ainsi que ceux qui contiennent des données sensibles après leur retrait d'exploitation

> **Date d'expiration du support technique des firmwares :** La page web de support technique de nombreux produits sur Axis.com stipule la date d'expiration du support technique du firmware de chaque produit. Les clients peuvent ainsi planifier la mise hors service et le remplacement d'un produit en temps opportun.

> **AXIS Device Manager Extend :** Cet outil permet de suivre facilement l'état de la garantie de tous les dispositifs du système, notamment par des informations sur la fin de production et de prise en charge des produits. Ces renseignements vous permettent de préparer un dispositif pour sa mise hors service et d'éliminer les risques associés à un dispositif dont le support technique n'est plus assuré.

> **Conseils :** Le portail AXIS OS du site web Axis fournit des conseils sur le retrait d'exploitation des dispositifs Axis. La remise aux paramètres d'usine d'un dispositif efface toutes les configurations et toutes les données.

Pour de plus amples informations, rendez-vous sur : **www.axis.com/fr/about-axis/cybersecurity**

© 2023 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC et VAPIX sont des marques déposées d'Axis AB dans différentes juridictions. Toutes les autres marques sont la propriété de leurs détenteurs respectifs.

AXIS COMMUNICATIONS