Recommandations en matière de cybersécurité de Dahua

Les risques de cyberattaque étant de plus en plus élevés envers les systèmes de vidéosurveillance, Dahua fournit des conseils et recommandations (disponibles sur notre site Web) pour renforcer au mieux la protection de votre système de sécurité.

Deux mesures obligatoires à prendre en matière de cybersécurité :

1. Utiliser des mots de passe forts et les modifier souvent

La principale raison du « piratage » des systèmes est l'utilisation de mots de passe vulnérables. Dahua recommande de créer un mot de passe fort chaque fois que c'est possible et de le modifier souvent. Un mot de passe fort est composé d'au moins 8 caractères et combine des caractères spéciaux, des chiffres, des majuscules et des minuscules.

2. Mettre à jour le micrologiciel

Comme c'est la norme dans les secteurs technologiques, nous recommandons de maintenir le micrologiciel des enregistreurs (NVR, DVR) et des caméras IP à jour afin de garantir que le système soit à niveau avec les correctifs de sécurité les plus récents. Vérifiez la version du micrologiciel de vos appareils fonctionnels. Si la date de version est obsolète de plus de 18 mois, veuillez contacter un distributeur local autorisé de Dahua ou l'assistance technique de Dahua pour vérifier la disponibilité d'une mise à jour de votre version.

* Dahua Technology a inséré la cybersécurité dans sa stratégie d'entreprise et s'efforce de fournir aux clients du monde entier des solutions et des produits sécurisés de manière positive, ouverte et coopérative. Pour les toutes dernières informations sur la cybersécurité chez Dahua, veuillez accéder à la page Web http://www.dahuasecurity.com/cybersecurity.html.

Dahua Mexique
Tél : +52 55 67231936
E-mail : sales.mx@global.dahuatech.com

Dahua Brésil
Tél : +55 11 32511871
E-mail : comercial.br@global.dahuatech.com

Dahua Thaïlande
Tél : +66 29382674
E-mail : info.th@global.dahuatech.com
hr.th@global.dahuatech.com

Dahua Corée du Sud
Tél : +82 7081618889
E-mail : DH-KOREA@global.dahuatech.com

Dahua Singapour
Tél : +65 65380952
E-mail : info.sg@global.dahuatech.com

Dahua Turquie
E-mail : sales.tr@global.dahuatech.com

Dahua Indonésie
E-mail : support.id@global.dahuatech.com
sales.id@global.dahuatech.com

Dahua Malaisie
Tél : +60376620731
E-mail : sales.mas@global.dahuatech.com

Dahua Inde
Tél : +91 1244569100
E-mail : sales.india@global.dahuatech.com

Dahua Russie
Tél : +7 (499) 682-60-00
E-mail : info@global.dahuatech.com

Dahua Kazakhstan
Tél : +7 727 3110838

Dahua Royaume-Uni
Tél : +44(0)1628 673 667
E-mail : sales.UK@global.dahuatech.com

Dahua Europe
Tél : +31 797999696

Dahua France
E-mail : sales.france@global.dahuatech.com

Dahua Espagne
Tél : +34 917649862
E-mail : sales.iberia@global.dahuatech.com

Dahua Italie
Tél : +39 3703446609
E-mail : sales.italy@global.dahuatech.com

Dahua Allemagne
E-mail : sales.de@global.dahuatech.com

Dahua CEE et pays scandinaves
Tél : +48 223957400
E-mail : biuro.pl@global.dahuatech.com

Dahua Afrique du Sud
E-mail : Dahua.sa@global.dahuatech.com

Dahua Australie
Tél : +61 299285200
E-mail : sales.oc@global.dahuatech.com

Dahua Moyen-Orient
Tél : +971 48815300
E-mail : sales.me@global.dahuatech.com

* La conception et les spécifications sont sujettes à changement sans préavis.

Centre de cybersécurité de Dahua - 01, janv. 2018

www.dahuasecurity.com

DAHUA TECHNOLOGY FRANCE
49 rue Auguste Perret, 94000 Créteil, France
Tél : 01 48 53 70 53
E-mail : sales.france@dahuatech.com support.france@dahuatech.com
www.dahuasecurity.com

Centre de cybersécurité de Dahua

Dahua Technlogy reconnaît les risques cybernétiques et est consciente de l'importance de la coopération avec les professionnels du monde entier pour améliorer la détection de la vulnérabilité et la cybersécurité de nos produits. C'est pourquoi nous avons créés le Centre de Cybersécurité Dahua (DHCC).

- **positif**
- **ouvert**
- **coopératif**

La cybersécurité est la protection des systèmes TI contre les vols et dommages apportés des matériels, logiciels ou informations de ces systèmes, et contre l'interruption ou le détournement des services qu'ils fournissent.

De l'influencer des élections au blocage des systèmes voire à l'extorsion envers des entreprises ou des individus pour des millions de dollars, les cybermenaces sont devenues plus fréquentes. La mise en œuvre accrue d'appareils réseau dans les systèmes de vidéosurveillance a modifié le paysage et constitue un nouvel ensemble de menaces pour le secteur de la sécurité matérielle.

Centre de cybersécurité de Dahua

Le DHCC a été fondé pour résoudre les problèmes de cybersécurité et a pour mission de fournir des solutions et des produits plus robustes et sécurisés à nos clients du monde entier. Ses fonctions sont la création de rapports de vulnérabilité de sécurité, de communiqués ou d'avis et de partager l'expertise en cybersécurité avec tous nos clients du monde entier.

Coopération avec les experts en cybersécurité

Dahua adopte une approche proactive consistant à consulter non seulement des partenaires réputés, tels que Synopsys Technology et DBAPP Security, mais également des agences gouvernementales chinoises et internationales spécialisées dans la cybersécurité. Dahua Technology se tient ainsi informée des toutes dernières menaces tant au niveau national qu'au niveau international.

DBAPP Security 安恒信息 · SYNOPSYS® · intel · UL

Produits et solutions de sécurité

Dahua a mis au point une gamme de produits de cybersécurité spécialisée dans son département de recherche et développement, et mis en place les outils de Synopsys pour résoudre les problèmes de qualité et de sécurité des logiciels, pour tous les produits sur tout le cycle de vie de développement de sécurité (SDLC) en utilisant plusieurs technologies, comprenant analyse statistique, test aléatoire et analyse de la composition logicielle. Dahua Technology participe aussi à la communauté BSIMM (renfort de la sécurité dans un modèle de maturité) et a déjà subi une évaluation BSIMM. Dahua a utilisé les résultats de l'évaluation BSIMM pour établir une mesure de référence de son programme de sécurité afin de ne cesser d'améliorer la qualité et la sécurité de ses produits au fil du temps.

Réponse à un incident de sécurité du produit

L'équipe de réponse à un incident de sécurité de produit de Dahua (PSIRT) est responsable de la réponse à donner dans ce cas. L'équipe PSIRT de Dahua est une équipe internationale dédiée dont l'objectif est de recevoir, d'enquêter et de communiquer publiquement les informations sur les problèmes et les vulnérabilités de sécurité relatives aux produits de Dahua. Dahua est membre du CNA (autorité chargée d'attribuer des codes CVE), permettant à la société de divulguer publiquement une vulnérabilité avec un identifiant CVE (exposition et vulnérabilité commune). Elle peut ainsi contrôler la divulgation des informations de vulnérabilité sans prépublication. Les matrices de risque emploient le système de classification de vulnérabilité commune (CVSS v 3.0) pour fournir des informations sur la gravité des vulnérabilités. Dahua promet de gérer chaque incident rapidement et de manière responsable et transparente.
Nous apprécions vos efforts pour nous aider à améliorer la cybersécurité des solutions et des produits de Dahua, et Dahua récompensera les utilisateurs qui auront signalé une vulnérabilité de sécurité après son évaluation.
Nous apprécions et encourageons vos efforts dans la détection et la signalisation des vulnérabilités, car cela nous aide à créer un monde connecté plus sûr et plus sécurisé.

Caractéristiques récentes relatives à la cybersécurité

Renforcement des mots de passe

Les utilisateur doivent désormais créer un mot de passe administrateur fort lors de l'initialisation de l'appareil. Dahua a également mis en œuvre des techniques de cryptographie, de lutte contre le cassage de mot de passe et des technologies de condensé de message pour empêcher les personnes les plus malintentionnées et les plus habiles de casser voire d'obtenir l'accès aux noms d'utilisateur et aux mots de passe.

Mise à niveau en ligne

Les utilisateurs ont la possibilité de mettre facilement à niveau à la version la plus récente du micrologiciel de sorte qu'ils puissent profiter des tous derniers correctifs de sécurité disponibles.