DIGITEMIS
CYBERSECURITY & PRIVACY

DAHUA - DHI-NVR4108/4116HS-8P-4KS2

CVE-2021-33046

DEFAUT DE CONTROLE D'ACCES

Bulletin de sécurité
21/01/2022

Romain KOSZYK (_ACKNAK_)

Description

I.1 PREREQUIS

Aucun prérequis n'est nécessaire. La vulnérabilité est exploitable par un attaquant non authentifié.

I.2 VULNERABILITE

Un défaut de contrôle d'accès permet de modifier l'adresse mail du propriétaire de l'enregistreur de vidéo Dahua sans être authentifié. Cette modification permet de réinitialiser ensuite le mot de passe du compte d'administration de l'équipement.

I.3 SCENARIO D'ATTAQUE

Nous présentons ci-dessous les différentes étapes qui ont permis d'exploitation cette faille qui affecte plus de 277 000 équipements exposés sur Internet.

La découverte partielle du mail de contact défini sur l'enregistreur vidéo peut se réaliser via l'appel à la fonction « *PasswdFind.getDescript* » :

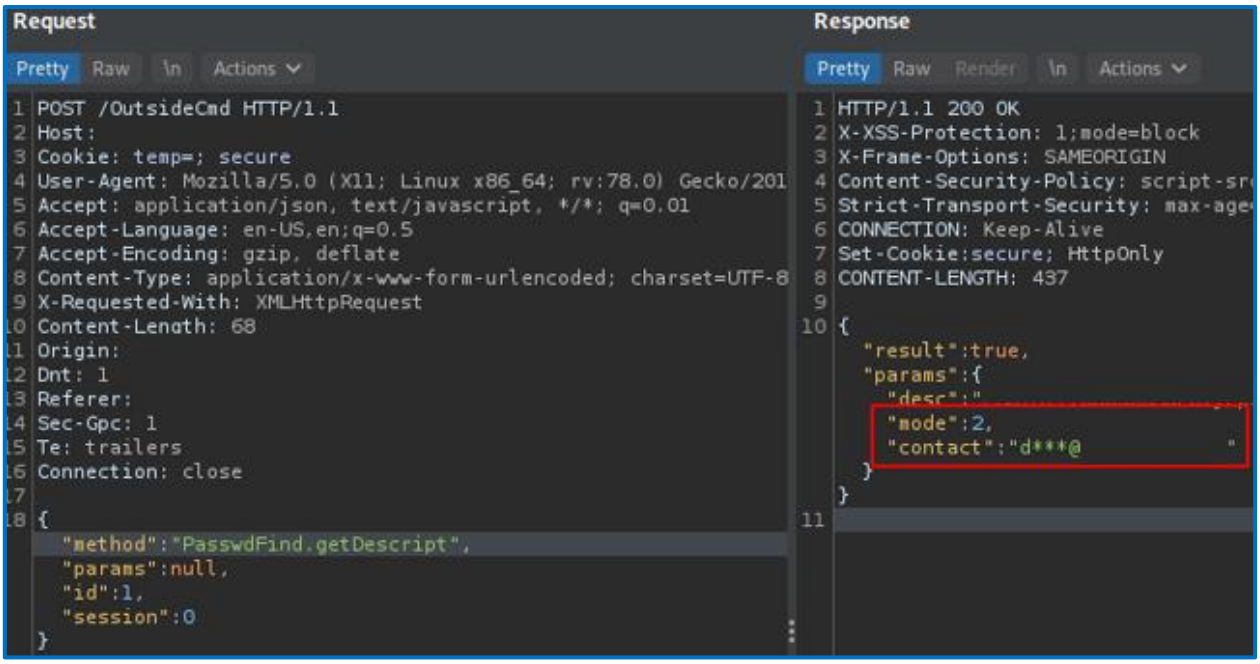


Figure 1 - Découverte partielle du mail de contact initialement défini sur l'équipement Dahua

On y découvre également un paramètre « *mode* » avec une valeur de 2.

Les fonctions relatives à la gestion du mail de contact dans le script « */app/jsCore/RPC.js* » sont les suivantes :

```
getContact:function(a){
  return a=a||0,b.send("PasswdFind.getContact",{
    mode:a
  }
  ).then(function(a){
    return a.params||{
    }
  }
  )
},
setContact:function(a,c){
  return b.encryptContentSend("PasswdFind.setContact",{
    mode:a,contact:c
  },
  "PasswdFind.setContact",null,"")
}
```

Figure 2 - Fonctions permettant de récupérer partiellement le mail de contact ou de le modifier

On remarque que la fonction « *getContact* » s'appuie sur la méthode « *send* » pour transmettre de la donnée, tandis que la méthode « *setContact* » repose sur la méthode « *encryptContentSend* ». Il est donc nécessaire de chiffrer les données de la méthode « *setContact* » afin de pouvoir interagir avec l'API associée.

La méthode « *encryptContentSend* » est décrite ci-dessous :

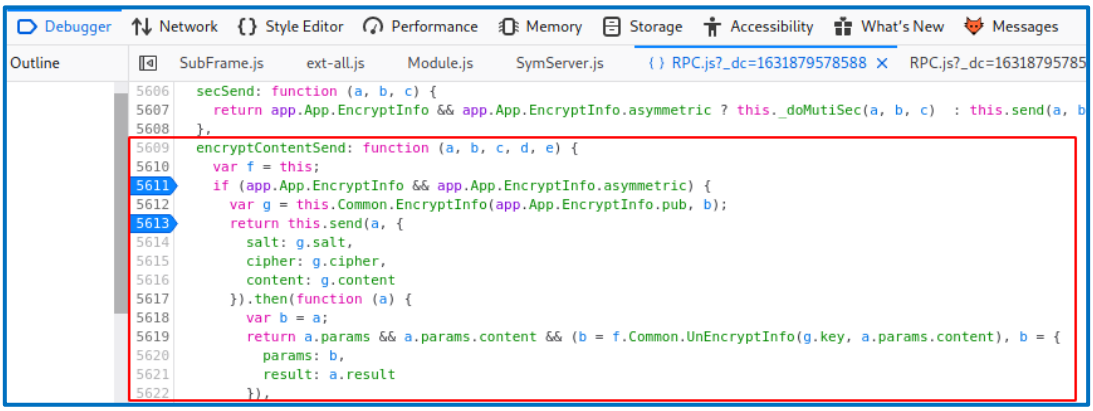


Figure 3 - Contenu de la méthode « encryptContentSend »

D'après la méthode « *setContact* », nous devons chiffrer l'objet suivant pour modifier le mail de contact :

```
{"mode":2, "contact":"romain.koszyk@digitemis.com"}
```

Figure 4 - Objet à chiffrer pour modifier le mail de contact de l'équipement

Nous avons défini des « *breakpoints* » dans le flux d'exécution du code JavaScript afin d'altérer la donnée à chiffrer avant qu'elle entre dans les différentes fonctions cryptographiques. Nous obtiendrons ainsi la donnée chiffrée à transmettre à la méthode « *setContact* ».

La méthode « *PasswdFind.checkAuthCode* » intervient lors de la soumission d'un code de sécurité dans la procédure de réinitialisation de mot de passe et chiffre les données saisies :

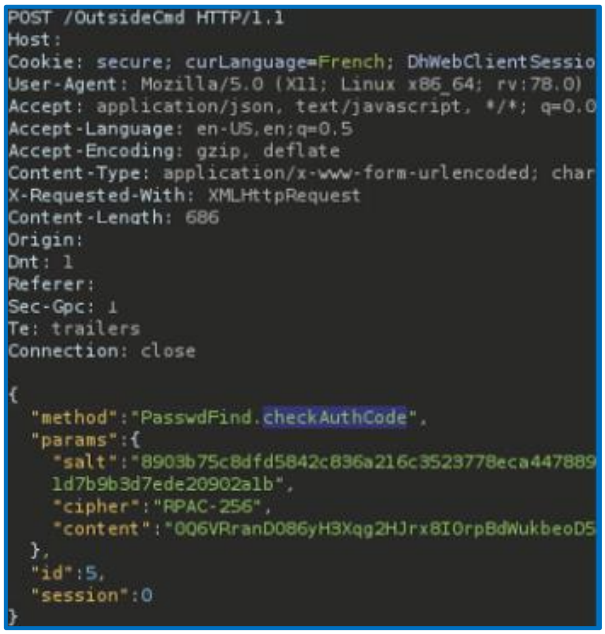


Figure 5 - Transmission de données chiffrées à l'API afin de vérifier le code de sécurité

Grâce aux « *breakpoints* » définis, nous allons altérer le flux d'exécution du code JavaScript associé :

Figure 6 - Mise en pause du flux d'exécution JavaScript lors de la saisie d'un code de sécurité, ici « some random input to be encrypted »

On constate qu'un objet contenant le code de sécurité saisie est présent dans la variable « *e* ». Nous allons modifier la variable « *e* » avant de reprendre le flux d'exécution du code JavaScript :

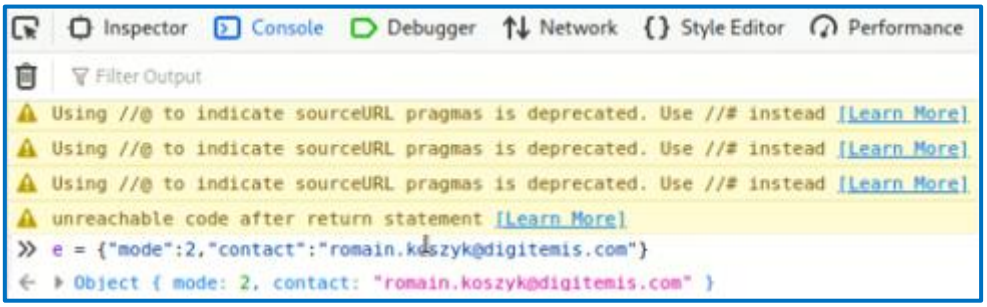


Figure 7 - Modification de l'objet afin de chiffrer les données nécessaires

Une pause dans le flux d'exécution une fois les données chiffrées nous permet de récupérer l'algorithme de chiffrement utilisé, le sel et le contenu chiffré de la variable « *e* » :

Figure 8 - Récupération des différentes valeurs cryptographiques nécessaires à la modification du mail de contact

Figure 9 - Requête de saisie du code de sécurité contenant les données chiffrées pour modifier le contact

La requête ci-dessus est invalide, car les données chiffrées ne correspondent pas à la méthode ciblée.

Nous renvoyons ces données avec la bonne méthode afin de modifier le mail de contact :

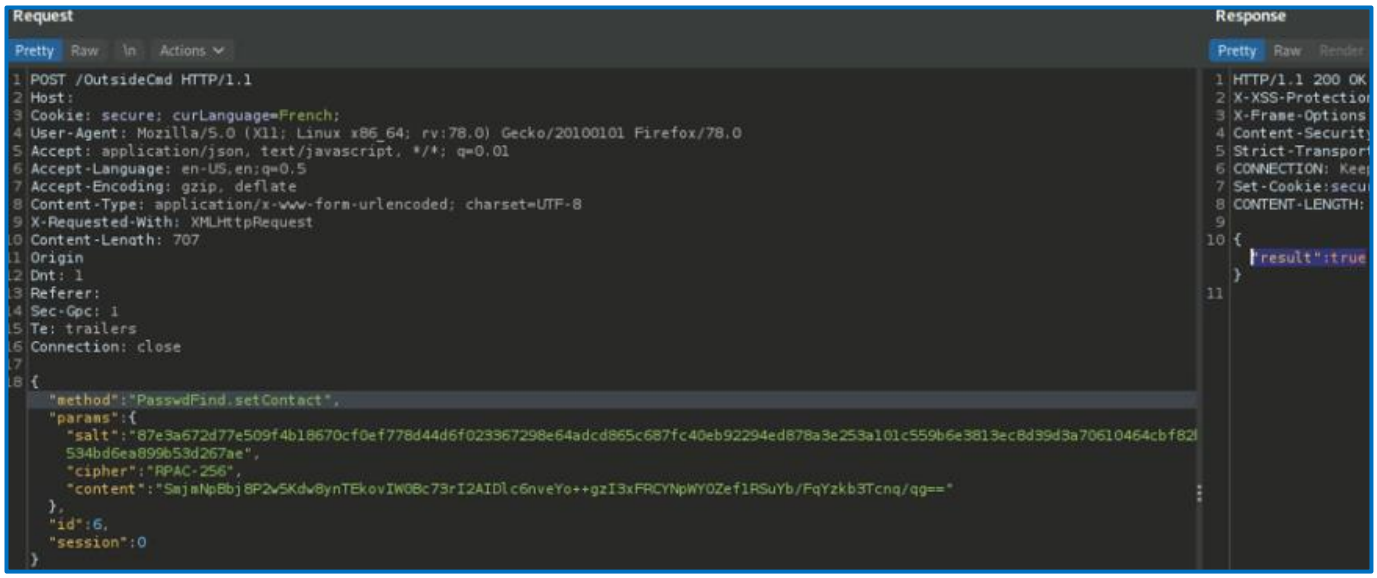


Figure 10 - Modification du mail de contact

On vérifie que le mail de contact a bien été altéré :

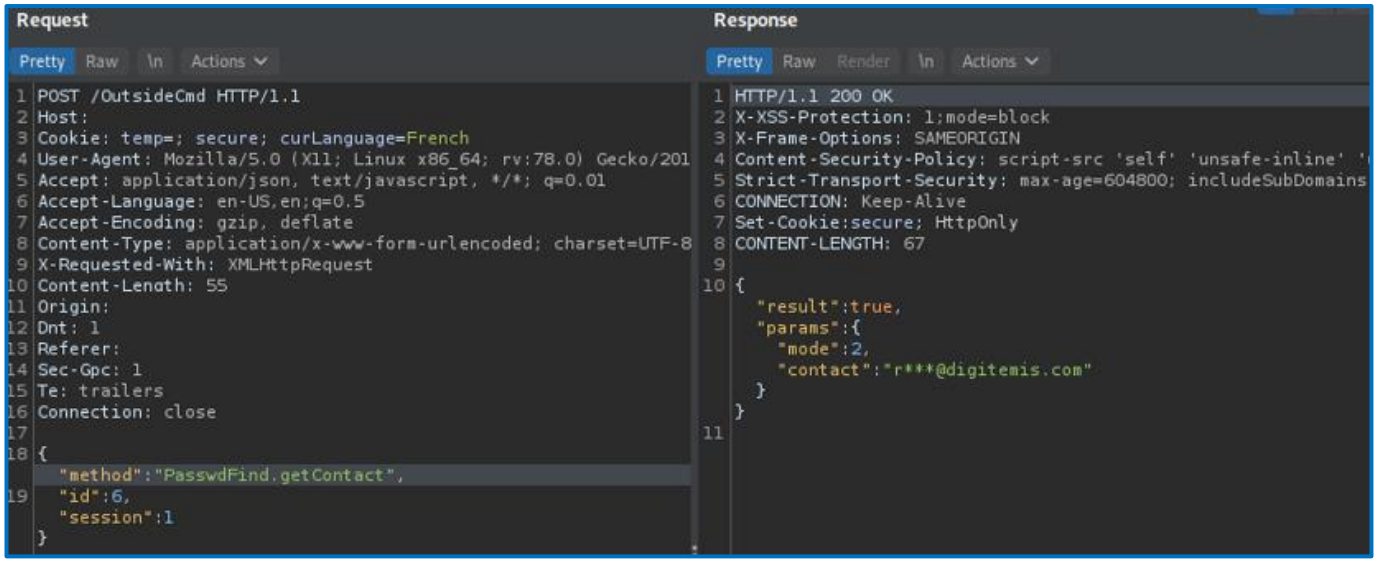


Figure 11 - Le mail de contact est modifié

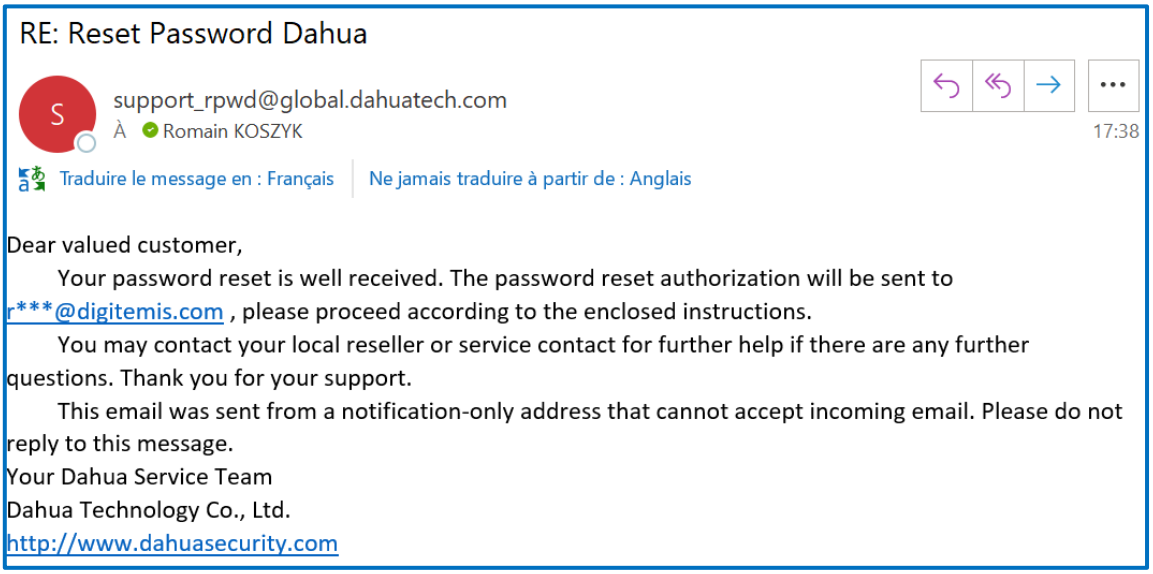
Il est alors possible d'entamer la procédure de réinitialisation de mot de passe de l'équipement.

Figure 12 - Procédure de réinitialisation de mot de passe du compte « admin » de l'enregistreur vidéo

Nous avons suivi la deuxième option de la procédure qui consiste à envoyer un mail à « *support_rpwd@global.dahuatech.com* » avec la donnée présente dans le QRCode :

Figure 13 - Envoi d'une demande de modification de mot de passe de l'équipement auprès de l'éditeur

5 minutes après, nous recevons 2 mails automatiques de la part du support. Le premier nous indique que le code de sécurité sera transmis au mail de contact défini dans l'équipement.


RE: Reset Password Dahua

support_rpwd@global.dahuatech.com
À Romain KOSZYK
17:38

Traduire le message en : Français | Ne jamais traduire à partir de : Anglais

Dear valued customer,

Your password reset is well received. The password reset authorization will be sent to r***@digitemis.com , please proceed according to the enclosed instructions.

You may contact your local reseller or service contact for further help if there are any further questions. Thank you for your support.

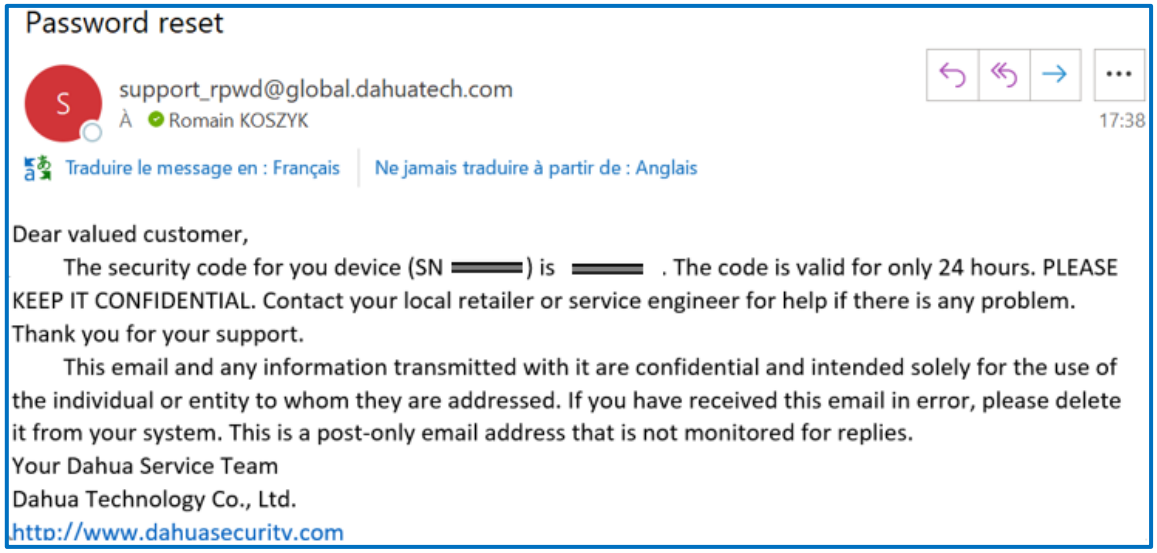
This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Your Dahua Service Team

Dahua Technology Co., Ltd.

http://www.dahuasecurity.com

Figure 14 - Mail automatique du support de Dahua (1/2)


Password reset

support_rpwd@global.dahuatech.com
À Romain KOSZYK
17:38

Traduire le message en : Français | Ne jamais traduire à partir de : Anglais

Dear valued customer,

The security code for you device (SN [redacted]) is [redacted] . The code is valid for only 24 hours. PLEASE KEEP IT CONFIDENTIAL. Contact your local retailer or service engineer for help if there is any problem. Thank you for your support.

This email and any information transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please delete it from your system. This is a post-only email address that is not monitored for replies.

Your Dahua Service Team

Dahua Technology Co., Ltd.

http://www.dahuasecurity.com

Figure 15 - Mail automatique du support de Dahua (2/2)

Nous disposons à présent du code de sécurité pour réinitialiser le mot de passe du compte « *admin* » de l'enregistreur vidéo.

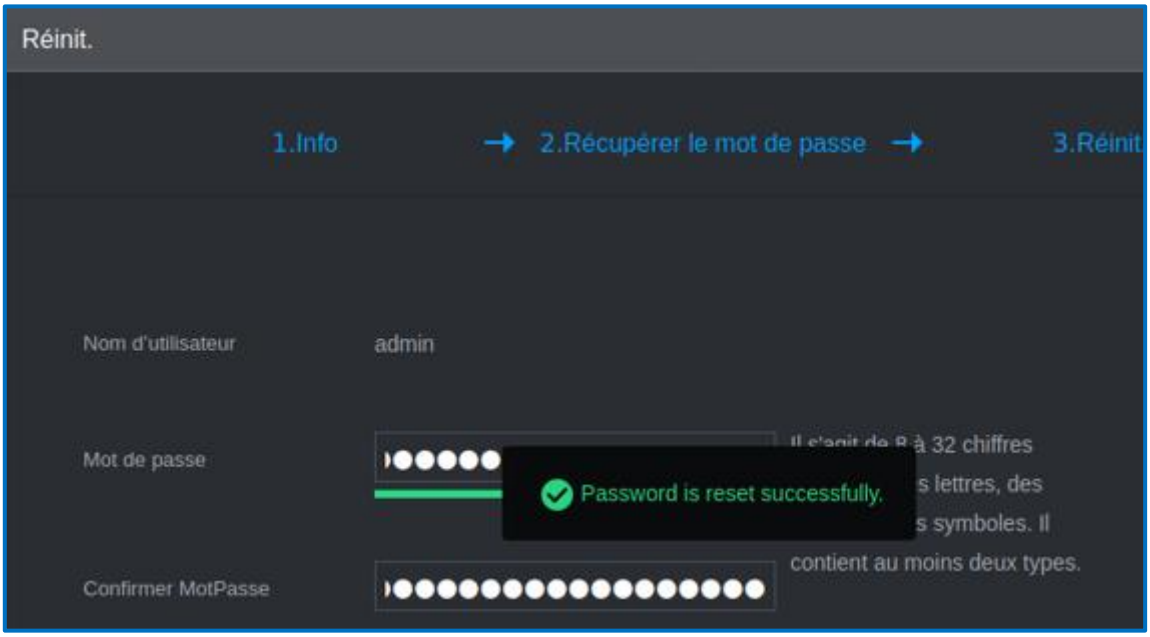


Figure 16 - Modification du mot de passe du compte « admin »

Nous pouvons ensuite nous connecter sur l'interface de gestion avec les privilèges d'administration.

Impacts & Risques

Un attaquant non authentifié peut prendre le contrôle de l'enregistreur vidéo.

Cette vulnérabilité a été identifiée sur la version 4.000.0000001.5.R.191218 de l'enregistreur vidéo DHI-NVR4108/4116HS-8P-4KS2. D'autres équipements et versions sont affectées comme décrits dans la publication du PSIRT de Dahua (« *https://www.dahuasecurity.com/support/cybersecurity/details/987* »).

Solution

Le contrôle d'accès sur la fonctionnalité de modification de l'adresse mail du propriétaire de l'enregistreur vidéo doit être systématique. Seuls les administrateurs authentifiés doivent être en mesure d'altérer une telle donnée.

Timeline

2021-09-16: Découverte de la vulnérabilité
2021-09-22: Envoi des details techniques à l'équipe de sécurité Dahua
2021-10-13 : L'équipe de sécurité de Dahua a confirmé la vulnérabilité
2021-11 : Mitre a affecté le numéro CVE-2021-33046
2021-01-12 : Dahua a publié un bulletin de sécurité avec les recommandations associées.

Référence

CVE : *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33046*
PSIRT Dahua : *https://www.dahuasecurity.com/support/cybersecurity/details/987*

Contact

romain.koszyk@digitemis.com