DIGITEMIS
CYBERSECURITY & PRIVACY

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

CVE-2021-33046

BROKEN ACCESS CONTROL

Security Advisory
21/01/2022

Romain KOSZYK (_ACKNAK_)

Description

I.1 PREREQUISITE

No prerequisites are necessary. The vulnerability can be exploited by an unauthenticated attacker.

I.2 VULNERABILITY

A broken access control allows to modify the email address of the owner of the Dahua video recorder without being authenticated. This change allows to reset the password of the administration account of the equipment.

I.3 ATTACK SCENARIO

Below are the different steps that allowed the exploitation of this flaw which affects more than 277 000 devices exposed on the Internet.

The partial discovery of the contact email defined on the video recorder can be done by calling the "PasswdFind.getDescript" function:

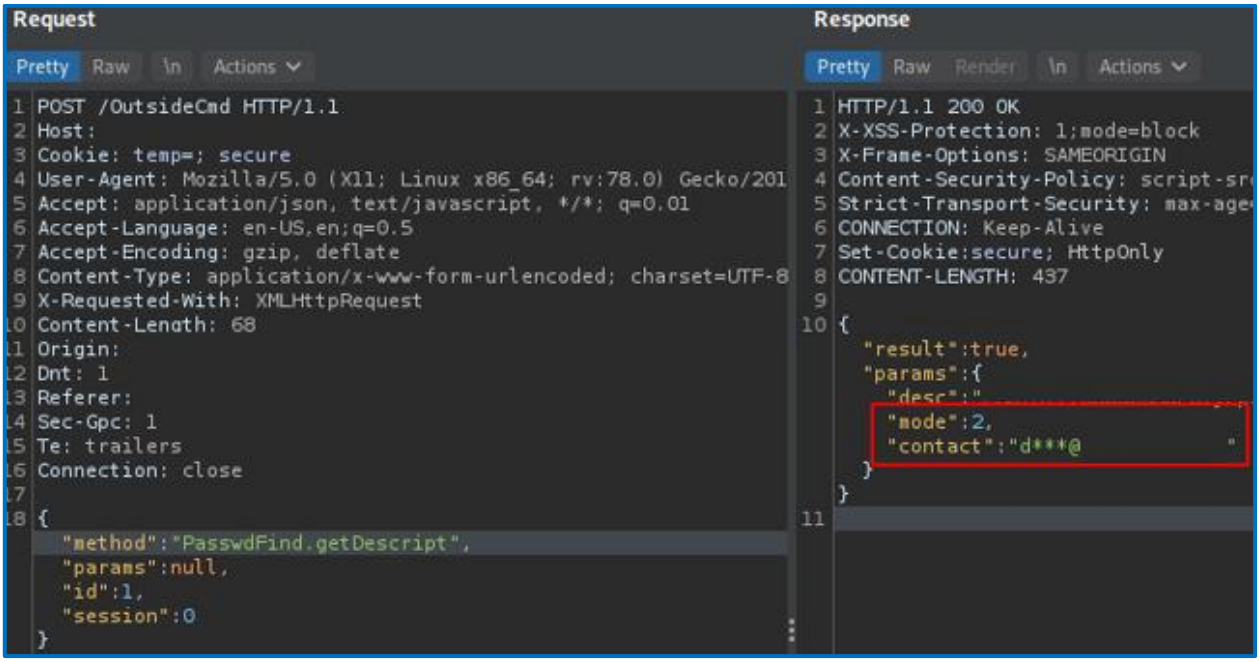


Figure 1 - Partial discovery of the contact mail initially defined on the Dahua equipment

There is also a "mode" parameter with a value of 2.

The functions related to the management of the contact mail in the "/app/jsCore/RPC.js" script are as follows:

```
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 - Functions allowing to partially recover the contact email or to modify it

We notice that the "getContact" function relies on the "send" method to transmit data, while the "setContact" method relies on the "encryptContentSend" method. It is therefore necessary to encrypt the data of the " setContact " method in order to interact with the associated API.

The " encryptContentSend " method is described below:

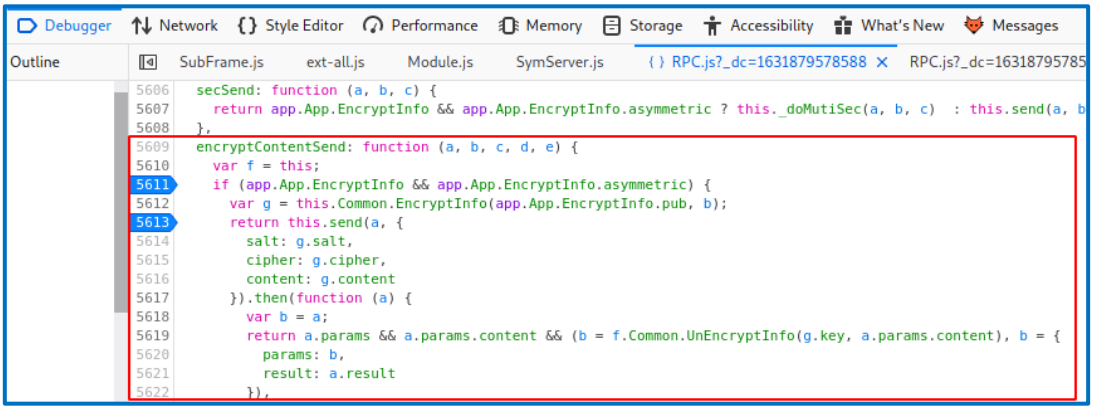


Figure 3 – Content of the « encryptContentSend » method

According to the "setContact" method, we need to encrypt the following object to modify the contact email:

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

Figure 4 - Object to be encrypted to modify the contact email of the equipment

We have defined "breakpoints" in the execution flow of the JavaScript code in order to alter the data to be encrypted before it enters the various cryptographic functions. We will thus obtain the encrypted data to be transmitted to the "setContact" method.

The "PasswdFind.checkAuthCode" method occurs when submitting a security code in the password reset procedure and encrypts the data submitted:

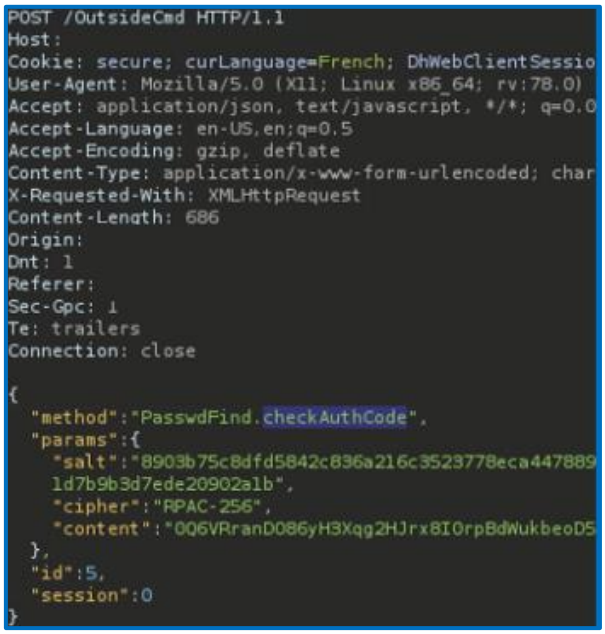


Figure 5 - Transmission of encrypted data to the API to verify the security code

Thanks to the defined breakpoints, we will alter the execution flow of the associated JavaScript code:

Figure 6 - Pause the JavaScript execution flow when entering a security code such as "some random input to be encrypted"

We can see that an object containing the submitted security code is stored in the "e" variable. We will modify the "e" variable before resuming the execution flow of the JavaScript code:

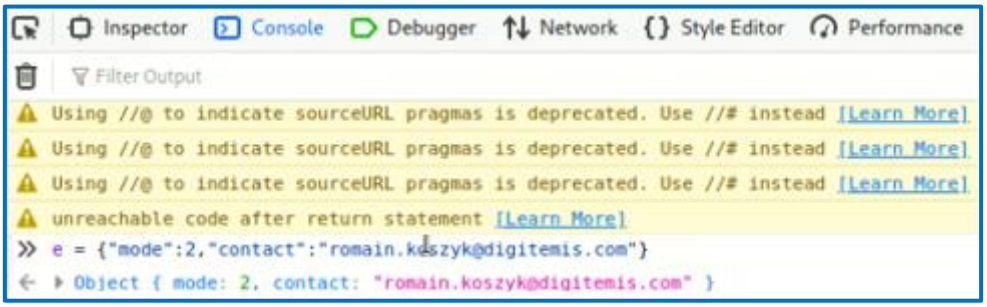


Figure 7 - Modification of the object to encrypt the necessary data

A pause in the execution flow once the data has been encrypted allows us to recover the encryption algorithm used, the salt and the encrypted content of the "e" variable:

Figure 8 - Recovery of the different cryptographic values required to modify the contact email

Figure 9 – Security code entry request containing the encrypted data to modify the contact

The above query is invalid because the encrypted data does not match the targeted method.

We return this data with the correct method to modify the contact email:

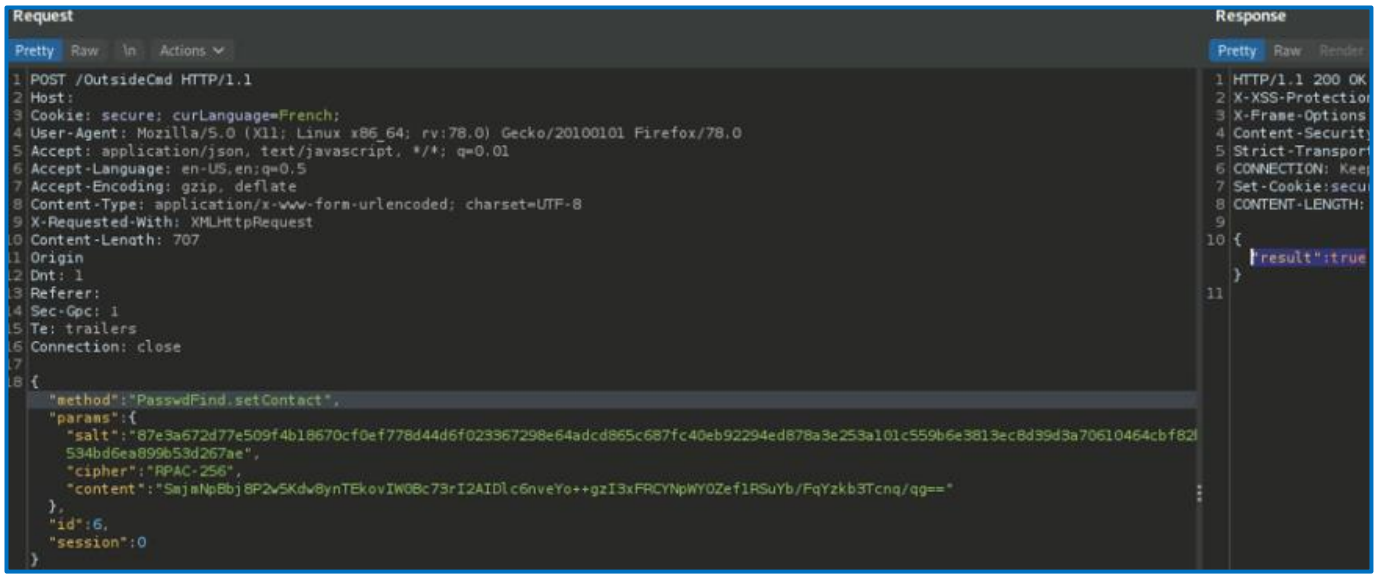


Figure 10 - Modification of the contact email

We check that the contact email has been changed:

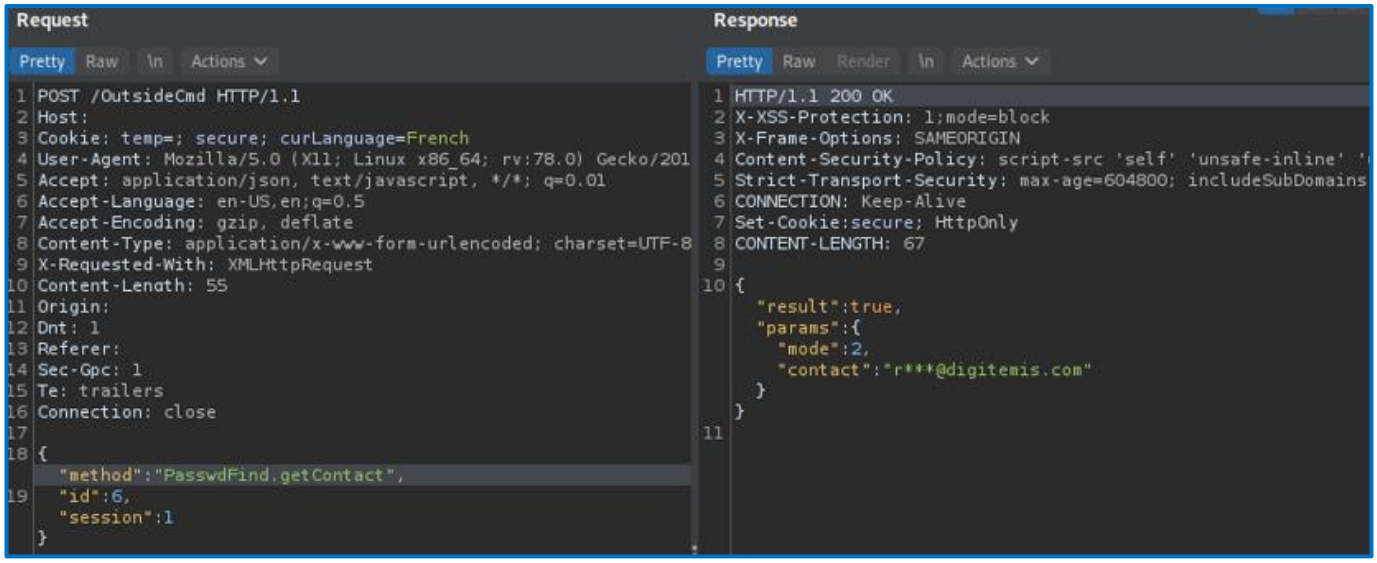


Figure 11 – The contact email has been changed

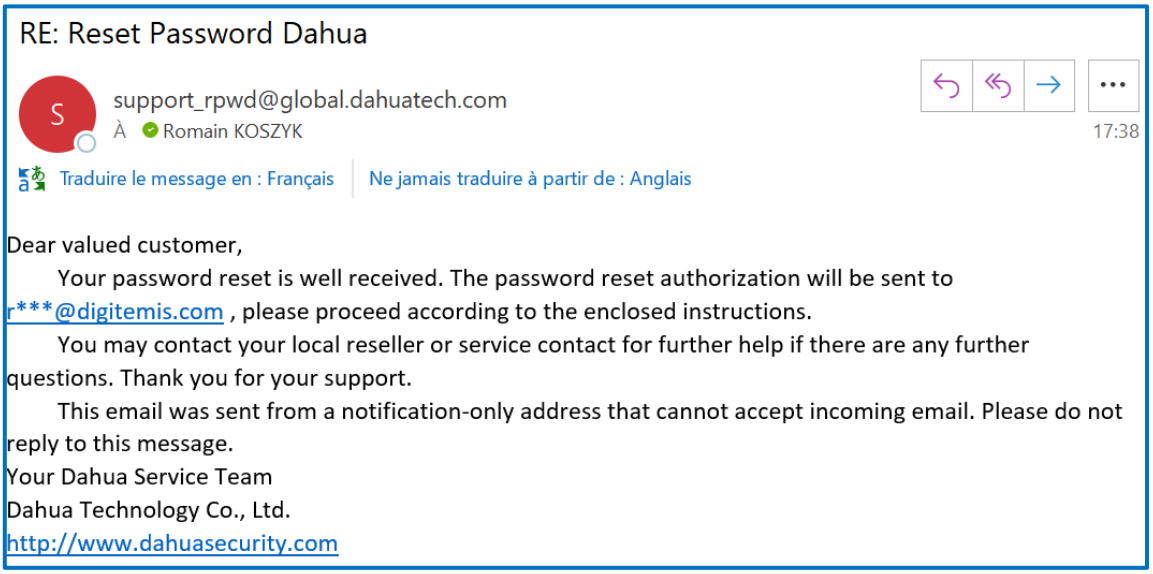
It is then possible to start the device password reset procedure.

Figure 12 - Procedure for resetting the password of the "admin" account of the video recorder

We followed the second option of the procedure which consists in sending an email to "support_rpwd@global.dahuatech.com" with the associated data of the QRCode:

Figure 13 - Sending a request to Dahua to change the password of the equipment owner

5 minutes later, we receive 2 automatic emails from the support. The first one tells us that the security code will be sent to the contact email defined in the equipment.


RE: Reset Password Dahua

S 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.

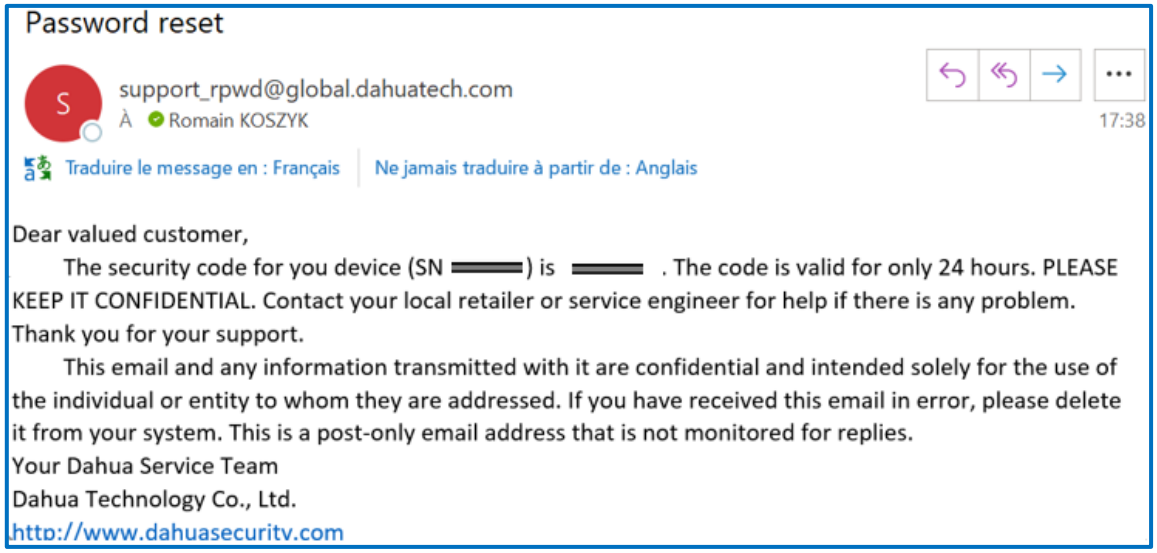
This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Your Dahua Service Team

Dahua Technology Co., Ltd.

http://www.dahuasecurity.com

Figure 14 - Automatic mail from Dahua support (1/2)


Password reset

S 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 - Automatic mail from Dahua support (2/2)

We now have the security code to reset the password for the "admin" account of the video recorder.

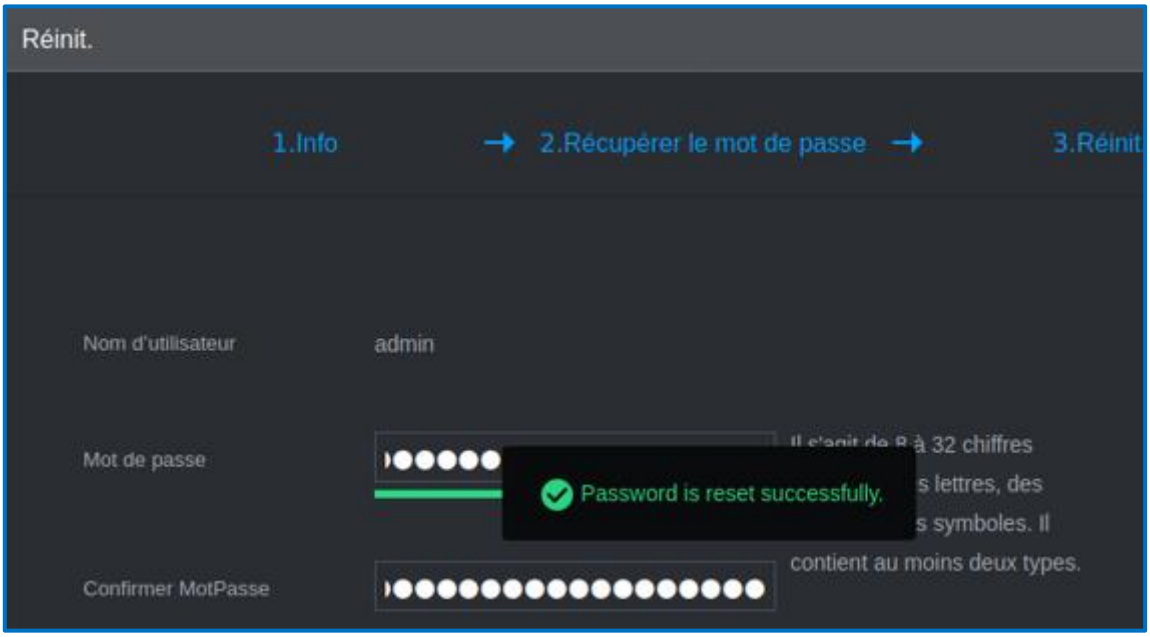


Figure 16 - Change the password of the "admin" account

We can then log into the management interface with administrative privileges.

Impacts & Risks

An unauthenticated attacker can take control of the video recorder.

This vulnerability has been identified in version 4.000.0000001.5.R.191218 of the DHI-NVR4108/4116HS-8P-4KS2 video recorder. Other devices and versions are affected as described in the Dahua PSIRT publication ("*https://www.dahuasecurity.com/support/cybersecurity/details/987*").

Remediation

Access control on the functionality to modify the email address of the owner of the video recorder must be enforced. Only authenticated administrators should be able to modify such data.

Timeline

2021-09-16: Discovery of the vulnerability
2021-09-24: Send full vulnerability details to the Dahua security team
2021-10-13: Dahua PSIRT confirmed the issue
2021-11: Mitre assigned CVE-2021-33046
2021-01-12: Dahua PSIRT published an advisory with detailed recommendations.

Contact

romain.koszyk@digitemis.com