SSD Advisory – Ichano AtHome IP Cameras Multiple Vulnerabilities

blogs.securiteam.com/index.php/archives/3576

Vulnerabilities Summary

The following advisory describes three (3) vulnerabilities found in Ichano IP Cameras.

AtHome Camera is "a remote video surveillance app which turns your personal computer, smart TV/set-top box, smart phone, and tablet into a professional video monitoring system in a minute."

The vulnerabilities found are:

- Hard-coded username and password – telnet
- Hard-coded username and password – Web server
- Unauthenticated Remote Code Execution

Credit

An independent security researcher, Tim Carrington, has reported this vulnerability to Beyond Security's SecuriTeam Secure Disclosure program.

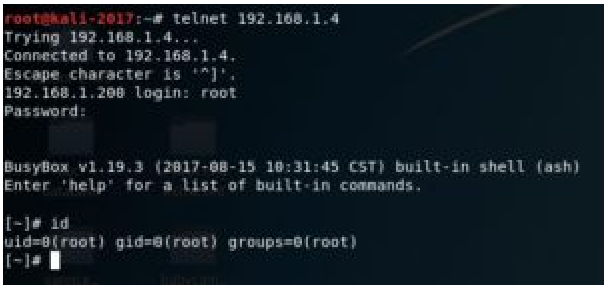
Vendor response

We tried to contact Ichano since November 21st 2017, repeated attempts to establish contact went unanswered. At this time there is no solution or workaround for these vulnerabilities.

<u>Vulnerabilities details</u>

Hard-coded username and password – telnet

The device runs a telnet server at startup with a default password of 123.



```
root@kali-2017:~# telnet 192.168.1.4
Trying 192.168.1.4...
Connected to 192.168.1.4.
Escape character is '^]'.
192.168.1.200 login: root
Password:


BusyBox v1.19.3 (2017-08-15 10:31:45 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

[~]# id
uid=0(root) gid=0(root) groups=0(root)
[~]#
```

Hard-coded username and password – Web server

In /app/www/doc/script/login.js, in the function DoLogin(), client side validation is used to login a user:

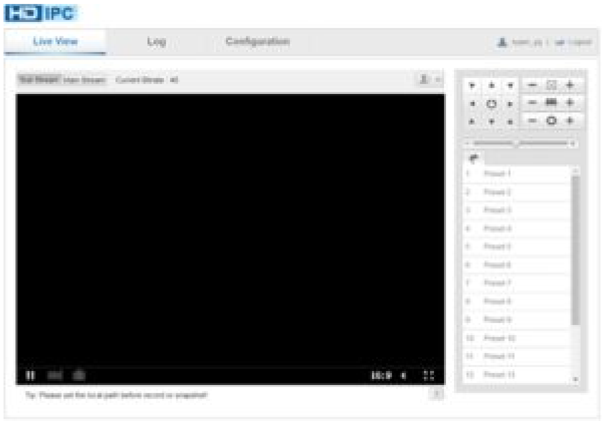
```
if($("#UserName").val()=="super_yg"){jumpPage();return}
```

A user can login with these credentials and can then take control of the device over http:

Unauthenticated Remote Code Execution

The device runs "noodles" binary – a service on port 1300 that allows a remote (LAN) unauthenticated user to run arbitrary commands.

The binary has a set of commands he can run – if a user will use the following “protocol”, command to be run is enclosed like html tags, i.e. <system>id</system>, a successful execution results in <system_ack>ok</system_ack>.



Tip: Please set the local path before record or snapshot!