Application Note

Internet Security for Barix Devices

1 Introduction

Recently news has reported that “…several stations using Barix Codecs for STL have been diverted to receive a hostile stream...“

A scary idea: Somebody hijacks your transmission and harms your brand reputation.

Some people talked about “hacking” others about “a security hole”. The reality was different: One did not need to be a professional hacker to take over these units because the door was very much open. A simple lookup on an Internet-of-things directory site revealed the unit, and then logging into it was easy with some of the units not having a password set, and others were entered by simply guessing the default password.

The following application note discusses how to minimize the danger of your units being controlled by other people.

2 Barix devices are secure

Barix devices are very secure. All except a few products run on a proprietary operating system that is highly unlikely to be the target of mainstream viruses. Secondly, they provide additional security settings within the firmware. Barix recommends reviewing your security settings and to address any potential weaknesses.

3 Set a strong password

Barix devices, dependent on the application they are configured for (Streaming Client, STL…), have no password set or have a default password. That is no problem, as long as the units run on a closed corporate network with no access from the outside world.

Like a lot of IP equipment, our devices are made and 95% are used in “friendly” local environments. If you install an IP phone, a printer, an appliance of some kind, they either have no or a default password installed. Typically, only routers, which are meant to connect to the outside world, are secured with a random password (and even there many are not).

The question is: Is your unit accessible from the World Wide Web?

For some applications and customers the remote access is a key feature and they plan for that. If you do so, you must set a strong password on the unit. In addition we recommend that you actually use a VPN (Virtual Private Network) to access your setup, instead of having the units directly connected to the Internet.

4 Could it be that your units are accessible without you even knowing?

Absolutely. When setting up an STL, one side needs to have a fixed IP address. It could well be that this IP address is public and your unit can be accessed from anywhere in the world. You might not even think about remote access, but in fact the unit is accessible using that fixed IP address.

Even worse: If a searchable URL is attached to this IP Address (like a web server) then it is easy for anybody to find out who the IP address belongs to, especially if the URL is www.your_radio_station_name.com.

For these reasons it is mandatory that you set a unique – non-obvious password for each device. Barix devices accept 24 character passwords.

5 Conclusions

5.1 Rule 1: Set or change to a strong password

What is a strong password:

Go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.

- Includes numbers, symbols, capital letters, and lower-case letters
- It shall not be a dictionary word or combination of dictionary words only
- It should not rely on obvious substitutions — for example, “Radi0transmitter” isn’t strong just because you’ve replaced an o with a 0.

5.2 Rule 2: Protect the web interface behind a firewall

Don’t use a public IP address that has a public web URL. Secure the web interface (port 80) behind a firewall with VPN capability.

Configure the firewall to port forwarding for the ports to which you are streaming. This way nobody can access the web interface unless he has your VPN password and your Barix device password. If you feel uncomfortable about firewall configuration, VPN and port forwarding, get an IP expert to assist you in setting up your network.

5.3 Rule 3: Use the STL firmware on the Barix device

The hijacking was not a Barix only problem. Other manufacturers are just as easy to hijack using the lookup on that Internet-of-things directory site as Barix was.

One reason why the Barix device was attractive was that these devices were probably running the Barix streaming client firmware instead of the STL firmware that was especially developed for radio broadcasters. Using streaming client (intended for internet radio reception) it is easy to put an http based stream as a source (a URL). The STL firmware made for broadcasters however does not support http based streaming, making the reconfiguring more complex. Running STL firmware does not protect the units from being hijacked, but it at least makes it less attractive. No matter what firmware is running, protection via access and password is a must.

6 Want even more security?

There is an option to outsource the concerns over the configuration of your Barix devices. Barix offers a save and secured deliver environment for audio delivery over the Internet without the need for local configurations and without exposing devices to the Internet, it is called **BARIX REFLECTOR SERVICE**.

The Barix broadcast Codec Exstreamer 500 comes preconfigured for that service. Customers intentionally need to reconfigure the devices for other uses.

With REFLECTOR all you have to do is to subscribe to the service that is operated and hosted by Streamguys (https://www.streamguys.com/services/cloud/reflector)

7 Summary

Barix devices are secure – as much as all other devices on the Internet – or in fact even more, because they run on a proprietary operating system that does not attract viruses. But it is with devices on the Internet like with your house: If you leave the door open, it is an easy game for people that have bad intentions.

Lock your door and if you can, build a gated community.

Do you have questions on your Barix devices? Need help with your settings?

Write to us at support@barix.com .

Barix AG
Ringstrasse 15A
8600 Dubendorf
SWITZERLAND

Phone: +41 43 433 22 11
Web: www.barix.com
Email: support@barix.com