7729 Pocoshock Way
N. Chesterfeld, VA 23235
Tel: 804-794-2500
www.avcomofva.com

Statement of Risk

Avcom of Virginia aims to produce test equipment that is functional without posing a risk to customer networks. There are currently no known security vulnerabilities with the Avcom EVO product family, however the product line has not been independently audited by security industry professionals. Despite the lack of formal data, use in the field suggests that the risk is low. Avcom products are used world-wide in a variety of industries in both the public and private sectors. Our company strives to follow industry best practices regarding product development and has made cautious design choices with the goal of reducing potential risk to customers. The following provides some background on the technologies used in the Avcom EVO product family in order to assist with threat modeling.

Firmware development for the Avcom EVO family of products is done entirely in-house in the United States. The firmware is built upon a custom embedded Linux distribution derived from technologies provided by the Yocto Project. At the time of writing, the distribution includes a variant of Linux 4.9.0 maintained by Analog Devices, Inc. and targets the ARMv7-A architecture. Since the distribution is built specifically for the application, additional software not related to the operation of the device is not included, reducing possible attack surface. Additionally, the application filesystem is loaded entirely into memory during power on and modifications do not persist between device reboots. Configuration options available to end users, such as device name and network settings, are stored on a separate non-volatile filesystem without executable permissions. Device firmware is field upgradeable through a USB flash drive and new firmware releases are offered regularly to enhance features, performance, and security.

As a network appliance, risk is often significantly lowered by applying appropriate network access controls. Network communication with the product family can, in the strictest sense, be limited to TCP port 26482, per default settings. Two UDP ports, 26482 and 26483, may additionally be used for device discovery and network reconfiguration. Since the reconfiguration protocol is not authenticated, it is recommended to restrict access to these ports to trusted systems at the risk of potential denial of service. Firmware releases do not include any services intended for remote shell access, such as Telnet or SSH, to reduce the risk of unauthorized control.

While there is not yet data regarding a concise risk rating from vulnerability scanning tools such as Nessus, suggestions for improving security posture and requests to mitigate any identified issues are always welcome. Please contact security@avcomofva.com to express any related concerns.