Multi-Domain RS-232 AV Control System Risk Management

Informative white paper requested by the Department of Defense community to provide an overview of increased Audio Visual RS-232 security risks in today's complex multi-domain classified Video Teleconferencing environments

March 20, 2020

AV Control System Risk Management
VTC CODECs

The majority of JITC approved VTC CODECs have a serial port which provides access to an extensive application programming interface (API). While recently released models may not have a physical serial port, the USB port can be used to access the same API. This API provides the ability to issue commands, read and write configuration settings, get current status, and be notified of events.

By default, the serial port requires authentication in the form of a username and password before external access is allowed. Initially, a CODEC is only configured with an administrator user role called "ADMIN", but additional user roles can be added, and a variety of permissions can be assigned to each one:

1. The USER role "can make calls and search the contact lists. The user can modify a few settings, e.g. adjust the ringtone volume and set the time and date format."
2. The AUDIT role can "change the security audit settings and upload audit certificates."
3. The ROOMCONTROL role can "create customized UI panels (for example in-room controls). This role has access to the UI Extensions editor and associated development [sic] tools."
4. The INTEGRATOR role has "access to settings, commands and status that are required to set up advanced AV scenarios, and to integrate our devices with third-party equipment. This role can also create customized UI panels."

When an external user authenticates via the serial port, they will have permissions for that session based on their role(s). However, the API variable "xConfiguration SerialPort LoginRequired" can remove authentication from the serial port entirely if set to "Off". In the "Off" condition, access to the serial port is nearly unrestricted, and external users will automatically have the role associated with the ADMIN role. For security reasons, this API variable is set to "On" by default, and can only be modified by an external user with the ADMIN role.

When the "SerialPort LoginRequired" variable is set to "On", the AV control system will be required to store a username and password in order to have access to the CODEC API. Consequently, the control system must provide a method for administrators to manage those credentials. The credentials stored in the AV control system processor must be kept in sync with the credentials required by the CODEC at all times to avoid disruption of service.

Storing the credentials of a CODEC attached to a production network in the AV control system processor dictates that the processor must adopt the classification (SECRET, TOP SECRET, etc.) of the CODEC's network. Even if the credentials are not stored inside the AV control system processor, standard security practices require the control system to adopt the classification level of the controlled equipment (due to the physical bi-directional serial connection). This makes programming and maintenance of the control system extremely challenging, as the computer being connected (or the AV LAN) must be at the same classification of the CODEC (or above). These issues are greatly compounded if the AV control system is used to manage multiple CODECs on multiple production networks of varying classifications.

In an attempt to alleviate these challenges the "SerialPort LoginRequired" variable is usually set to "Off". While this undoubtedly makes support and management easier, it also creates security vulnerabilities. Disabling serial port authentication provides unrestricted access via a physical bi-directional connection to the CODEC.

There is a common misconception that the serial port does not allow “network access” from an external user/device, meaning that the serial port only allows you to configure the CODEC, perform basic tasks, and check its status. While it is true that you cannot route packets via the serial port, the serial API does provide the ability to access the production network that the CODEC is connected to.

The most complete method of network access was introduced in version CE9.6 of the API. The “xConfiguration HttpClient” variables allow serial port users to fully consume the HTTP services of the network to which the CODEC is connected to. Users could, for example, search web servers for keywords and then store matching data on other servers. Anything possible from a web browser on that network is essentially possible from the serial port of a CODEC attached to that network. It’s vital to note these commands are only accessible to ADMIN users, and therefore should never be available to an AV room control system. However, systems in which the “SerialPort LoginRequired” variable is set to “Off” are providing such capabilities to the AV control system de facto. While it is true these commands can be disabled, the ADMIN role to which the control system has access can simply re-enable them. These API commands could be used to move data across networks.

This type of attack via the serial port is viable for data exfiltration in multi-domain, single CODEC systems, where the CODEC may only be physically connected to one network at a time, or in multi-CODEC systems, where only one CODEC is active at a time. Disconnecting un-used CODECs from their production networks or enabling/disabling inputs and outputs will not mitigate this risk. A malicious or compromised AV control system could perform the attack asynchronously, downloading data from one network while active, and then waiting for another network to become active before posting that data.

It’s not only ADMIN users who can access the network via the serial port of the CODEC. Other user roles can also utilize this potential avenue of attack. For example, USER and INTEGRATOR roles can access the “UserInterface Branding Fetch” command, which is intended to allow a system to pull down images to the CODEC. While it is very safe for that purpose, a potential attacker could use that command to make an HTTP GET request to any URL they choose, which could have security implications for poorly coded web servers (a common vulnerability). The command could also be used for network probing or data exfiltration. That command is only an example. There are other system URLs and network information data which can be set by non-ADMIN users, which may serve as attack vectors on the network that the CODEC is connected to.

It is clear from the issues outlined above that the CODEC serial port should require authentication as intended by the manufacturer, and that the user account provided to AV control system should not have ADMIN privileges. To do so otherwise is a violation of NIST SP 800-53v4 Account Management (AC-2) and Access Enforcement (AC-3), which are required for even low impact systems.

In addition, the AV control system should be connected to the CODEC via an isolation device that restricts bi-directional communication via the serial port. Such a device can prevent the control system from retrieving sensitive data from the CODEC and/or the production network it is connected to. It can also provide a standard COTS solution for credential management. Such a device can also provide for the fine tuning of allowable serial API commands, denying commands that might be malicious, or only allowing approved commands, in accordance with the principle of least privilege.