CRESTRON NVX SECURITY GUIDE

Crestron Electronics, Inc.

REVISION HISTORY

Version	Date	Comments	Author(s)
1.00	October 9, 2018	Initial Version	JP
1.01	January 18, 2019	Added Autodiscovery Instructions	JD, JP, MR

1 OVERVIEW

For a number of years now, Crestron has been designing systems with a focus on integration into and along with Enterprise IT infrastructure. Support for Active Directory, 802.1x and SNMP, as well as a shift to industry standard protocols including support for SSH and the latest versions of TLS, is a top priority. Products are rigorously tested to ensure stability and compatibility within the Enterprise.

A large part of this is designing systems with security in mind. Part of the U.S. Department of Defense, the Joint Interoperability Test Command (JITC) conducts testing for network devices on behalf of the U.S. Military. Security functions are of course the highest priority, but testing also touches on interoperability and other operational functionality. While focused on the needs of the DoD and other federal agencies, the test criteria are applicable to any professionally managed enterprise.

2 DEVICES

This document describes the security aspects of the Crestron NVX which is built on Linux.

In particular the following models are covered by this document.

Model	Firmware Version	OS Version	OpenSSL Version
DM-NVX-350 DM-NVX-351 DM-NVX-350C DM-NVX-351C	1.3707.00028	Linux (4.1.0+)	OpenSSL 1.0.1p

While Crestron NVX is built on "Linux," they are fundamentally different devices than the Linux devices the reader may be more familiar with.

- Lack of access to a standard desktop or user shell as well as no wireless communications significantly reduces the number of relevant vulnerabilities.
- The devices support 802.1X authentication.

3 SECURITY

The encryption libraries in Crestron NVX are provided via OpenSSL rather than the stock Android encryption methods.

Crestron also regularly reviews the National Vulnerability Database and Common Vulnerabilities and Exposures Database for any applicable security flaws and makes certain that any required patches are given the highest possible priority and provided to all customers free of charge.

In addition, the platform is patched during any regularly scheduled firmware update.

4 SECURE DEPLOYMENT INSTRUCTIONS

To harden any of the devices referenced in this document, please use the following commands.

- `AUTHENTICATION ON`
- `SSL NOVERIFY`
- If talking to a control system with Authentication on (in the control system), supply user/password for the control system CIP connection via `SETCSAUTHENTICATION` command.

The NVX also includes a web server for configuration which can be disabled with the following command. However, the web server does use authentication, encrypted communications and is needed for stream routing functionality.

- `WEBSERVER OFF`

Turning on Authentication automatically disables the FTP server, Telnet access and CTP (legacy Toolbox console). The commands below are simply added for completeness.

- `FTPSERVER OFF`
- `TELNETPORT OFF`
- `CTPCONSOLE DISABLE`

If 802.1X features are required, they may be configured using the web browser.

Crestron devices support an autodiscovery feature which allows them to be detected, report basic information, and do some basic configuration remotely. This feature is not protected by authentication; therefore, this feature should be disabled for improved security.

Autodiscovery can be shut off by using the following command:

- `AUTODISCOVERY OFF`