CRESTRON TOUCHSCREENS SECURITY GUIDE

TSW-X52 TSW-X60 DGE-X00 TS-1542X

Crestron Electronics, Inc.

REVISION HISTORY

Version	Date	Comments	Author(s)
1.00	March 7, 2018	Initial Version	JP
1.01	March 9, 2018	Added DGE and TS touchscreens	JP
1.02	March 12, 2018	Release Version	JP
1.03	May 23, 2018	Added 802.1X Reference	JP
1.04	January 18, 2019	Added Autodiscovery Instructions	JD, JP, MR

TABLE OF CONTENTS

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.

The Crestron touchscreens in this document are a part of the Crestron video distribution systems that are currently listed on the Approved Products List. NOTE: The listing for the TSW-x60 family targets the -NC (no camera) versions of the product but the security functionality is otherwise the same.

2 DEVICES

This document describes the security aspects of the Crestron TSW touchscreens which are built on Android.

In particular the following models are covered by this document.

Model	Firmware Version	OS Version	OpenSSL Version
TSW-552	1.003.0020	Android ICS (4.0.4)	OpenSSL 1.0.1l
TSW-752			
TSW-1052			
TSW-560	1.002.0031	Android Lollipop (5.1.1)	OpenSSL 1.0.1l
TSW-560P			
TSW-560-NC			
TSW-760			
TSW-760-NC			
TSW-1060			
TSW-1060-NC			
TS-1542	1.3384.00049	Android ICS (4.0.4)	OpenSSL 1.0.1l
TS-1542-C			
DGE-100			
DM-DGE-200	1.3384.00049	Android ICS (4.0.4)	OpenSSL 1.0.1l

While Crestron TSW touchscreens are built on "Android," they are fundamentally different devices than the Android devices the reader may be more familiar with.

- There is no access to the Google Play Store or any method to allow arbitrary 3rd party applications to run on the device.
- While the devices do include a browser client, this is typically not exposed to the end user. And in typical use when it is exposed, it is usually set to render a captive URL and no browsing to arbitrary URLs is provided. This is fully within the installer's control.
- The lack of wireless communications significantly reduces the number of relevant vulnerabilities. Bluetooth is only used for beaconing support.
- The Crestron TSW touchscreens designated as -NC have no camera, microphone or Bluetooth beacon support.
- The devices support 802.1X authentication.

3 SECURITY

The encryption libraries in Crestron TSW touchscreens 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.
- If SIP/RAVA support is not needed you can disable it with the command `SIPENABLE OFF`. SIP over TLS is also supported if desired.
- `ENTERSETUPSEQ DISABLE`

The x60 family of devices also includes a web server for configuration which can be disabled with the following command.

- `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`

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`