TTCR 14.1

Build cybersecurity defense

Cybersecurity is one of the growing concerns in the industry that can impact plant operations. Proper maintenance of your turbomachinery control systems is key to minimizing cybersecurity risks. TTCR 14.1 is a packaged release of critical system components focused on improving cybersecurity defense around your turbomachinery.

The process of upgrading to TTCR 14.1 is seamless and will not cause data loss or process disruptions. Your familiar HMI will continue to operate the same way with additional layer of cybersecurity defense in place.

Secure your CCC turbomachinery control systems with Total Train Comprehensive Release (TTCR) 14.1

CCC utilizes the industry-recognized Nessus™ Vulnerability Scanner to systematically identify vulnerabilities during and after TTCR development. Vulnerability identification test in accordance with SSA-420 has identified no vulnerabilities of LOW or higher on TrainTools server running on TTCR 14.1.

Upgrade seamlessly without disruptions

For customers with existing TrainTools servers running under older TTCR versions, the upgrade process to 14.1 is seamless and easy. The new release retains the familiar look and feel – requiring no additional training – while improving your system security. TTCR 14.1 upgrade is also a perfect opportunity to address obsolescence of Windows® operating system and PC hardware. Qualified CCC engineers will help you identify the right upgrade path and test the new system to assure full solution performance.
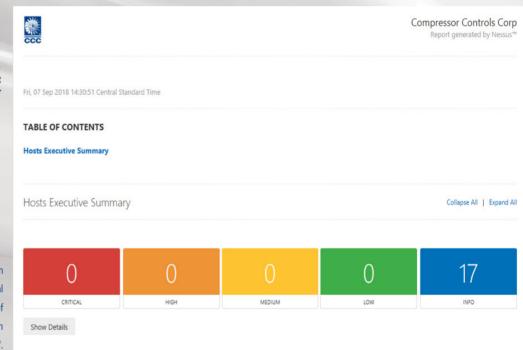
Security improvements

- Upgraded Firebird™ SQL server and other third-party dependent libraries

- Improved TrainTools User Accounts password complexity requirements

- Improved TrainTools Diagnostics Utility for one-click comprehensive system diagnostics

- Support for the latest Windows OS versions as well as VMware virtualization

Other enhancements

- Added support for dedicated Ethernet ports for communication with third-party systems (Prodigy®)

- Added support for floating point Modbus registers (Prodigy)

Platforms

TrainTools / TrainView
Series 3 Plus, Series 3++, Series 5 Vanguard®, Series 5 Reliant, Series 5M, Prodigy

▶
TrainTools Server Scan Report using Nessus Vulnerability Scanner

* Utilizing Nessus Vulnerability Scanner configured in accordance with ISA Secure® SSA-420 standard with all typical system services running and hardening applied. Report as of September 7, 2018. CCC has no affiliation with ISASecure® or Tenable®.

Compressor Controls Corp
Report generated by Nessus™

Fri, 07 Sep 2018 14:30:51 Central Standard Time

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary   Collapse All | Expand All

0	0	0	0	17
CRITICAL	HIGH	MEDIUM	LOW	INFO

Show Details

For additional information visit: www.cccglobal.com

Expertise In Turbomachinery Optimization

CCC®