Life Is On Schneider Electric

Schneider Electric Security Bulletin

Legacy Triconex™ Product Vulnerabilities (V2.1)

14 April 2020 (23 June 2020)

Overview

Before being acquired by Schneider Electric, the then-Invensys Triconex brand team discovered and remediated multiple vulnerabilities affecting legacy versions of the company's Triconex brand safety instrumented system offer, following company processes and procedures in place at that time. The vulnerabilities affected:

- TriStation™ 1131 v1.0 to v4.9.0, and v4.10.0 to 4.12.0 operating on Windows® NT, Windows XP or Windows 7
- Tricon™ Communication Module (TCM) Models 4351, 4352, 4351A/B and 4352A/B installed in Tricon v10.0 to v10.5.3 systems

Customers were then notified of updated product availability via direct-to-customer notification. See the table in the "Available Remediations" section below for links to the release notifications (registration required).

Fixed versions of these offers are available for download here:
https://pasupport.schneider-electric.com/

In 2019, an independent researcher notified Schneider Electric of these same vulnerabilities. As part of its strong commitment to being as open, transparent and collaborative as possible to help its customers and global industry prevent and respond to potential cybersecurity threats and vulnerabilities, Schneider Electric, in collaboration with MITRE CVE and the independent researcher, has issued CVE® (Common Vulnerabilities and Exposures) Entries for these previously identified and fixed product vulnerabilities.

Users of current and more recent versions of the identified firmware and software offers are not exposed to these specific vulnerabilities. Schneider Electric continues to urge customers always to implement and adhere to the instructions provided in the "Security Considerations" sections of customers' Triconex documentation (*Planning and Installation Guides* and *TriStation 1131 Developer's Guide*) and *Triconex System Security Reference Guide*. The company also strongly recommends upgrading to the latest versions of Microsoft® Operating Systems, including updating to the newest Windows platforms that host Triconex software.

If interested, see below for more information about these vulnerabilities.

Schneider Electric Security Bulletin

Details

CVE ID: **CVE-2020-7483**

A vulnerability related to the "password" feature in TriStation 1131 versions 1.0 through 4.12.0 could cause certain data to be visible on the network when the feature was enabled. This vulnerability was remediated in version 4.13.0.

CVE ID: **CVE-2020-7484**

A vulnerability related to the "password" feature in TriStation 1131 versions 1.0 through 4.12.0 could allow a denial of service attack if the user is not following documented guidelines pertaining to dedicated TriStation 1131 connection and key-switch protection. This vulnerability was remediated in version 4.13.0.

CVE ID: **CVE-2020-7485**

A vulnerability related to a legacy support account in TriStation 1131 versions 1.0 through 4.9.0 and 4.10.0 could allow inappropriate access to the TriStation 1131 project file. This vulnerability was remediated in TriStation 1131 versions 4.9.1 and 4.10.1.

CVE ID: **CVE-2020-7486**

A vulnerability could cause TCMs installed in Tricon system versions 10.0.0 through 10.4.x to reset when under high network load. This reset could result in a denial of service behavior with the SIS. This vulnerability was remediated in TCM version 10.5.0.

CVE ID: **CVE-2020-7491**

A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4.

Available Remediations

Fixed versions of these offers are available for download here:
https://pasupport.schneider-electric.com/

CVE ID	Product	Affected Versions	Fixed Version (link to Product Release Notice)	Fixed Version Release Date
CVE-2020-7483	TriStation 1131	v1.0 to v4.12.0	v4.13.0	1/26/2015
CVE-2020-7484	TriStation 1131	v1.0 to v4.12.0	v4.13.0	1/26/2015
CVE-2020-7485	TriStation 1131	v1.0 to v4.9.0 and v4.10.0	v4.9.1 and v4.10.1	5/30/2013
CVE-2020-7486	Tricon TCM Model 4351, 4352, 4351A/B, 4352A/B	v10.0.0 to v10.4.x	v10.5.0	08/13/2009
CVE-2020-7491	Tricon TCM Model 4351, 4352, 4351A/B, 4352A/B	v10.2.0 to v10.5.3	v10.5.4	02/02/2012

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls, so unauthorized personnel are unable to access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Scan all methods of mobile data exchange with the isolated network, such as CDs, USB drives, etc., before use in the terminals or nodes connected to these networks.
- Never allow laptops that have previously connected to any network other than the security or control networks to connect to those networks without proper sanitation.

- Minimize network exposure for all control system devices and systems, and verify that they are never accessible from the internet.
- When remote access is required, use secure methods, such as Virtual Private Networks. Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, recognize that VPNs are only as secure as the connected devices.

Schneider Electric continues to recommend customers always implement the instructions in the "Security Considerations" sections of the provided user documentation, which include the following:

- Verify that the cybersecurity features in Triconex solutions are always enabled.
- Always deploy safety systems on isolated networks.
- Secure all TriStation engineering workstations and never connect to any network other than the safety network.
- Configure operator stations to display an alarm whenever the Tricon key switch is in the "PROGRAM" mode.

Cybersecurity Preparedness:

- Review and assess your site's cybersecurity preparedness. Schneider Electric is a proponent of the NIST Cybersecurity Framework and is ready to assist.
- The Schneider Electric Product Security Office continues to work with ICS-CERT and will update this advisory as more information becomes available.
- Always refer to the Global Customer Support website for the latest list of Triconex security recommendations, or contact your local Triconex representative.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

Schneider Electric Security Bulletin

Revision Control:

Version 1 *14 April 2020*	Original Release
Version 2 *12 May 2020*	Added CVE CVE-2020-7491 and updated affected versions for CVE-2020-7483, CVE-2020-7484, CVE2020-7485 (page 2-3)
Version 2.1 *23 June 2020*	Updated overview, affected versions, fixed versions, and CVE descriptions (page 1-3)

Product Security Office

Digitally signed by Product Security Office
Date: 2020.07.15 13:59:20 -04'00'