Schneider Electric Security Notification

Triconex Models 3009/3009X MP, 4351B/4352B/4355X TCM, and 4610X UCM (V1.1)

11 May 2021 (13 July 2021)

Overview

Schneider Electric is aware of multiple vulnerabilities in its Triconex™ Tricon™ Main Processor (MP), Tricon Communication Module (TCM), and Unified Communication Module (UCM) products.

The affected products (listed below) are main processor modules and communication modules intended for use with Tricon and Tricon CX systems.

Failure to apply the remediations provided in this document may risk a denial of service attack, which could result in a module reset.

July 2021 update: Improved additional mitigations related to the write-protect keyswitch and clarified affected modules.

Affected Products and Versions

The following modules when installed in Tricon or Tricon CX version 11.3.x – 11.7.x systems are affected:

- Tricon Main Processor Models 3009 and 3009X
- Tricon Communication Module (TCM) Models 4351B, 4352B, and 4355X
- Unified Communication Module (UCM) Model 4610X

Vulnerability Details

CVE ID: **CVE-2021-22742**

CVSS v3.1 Base Score 3.9 | Low | CVSS:3.1/AV:P/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists in the Model 3009/3009XMP that could cause a module reset when the TCM receives malformed TriStation packets while the write-protect keyswitch is in the PROGRAM position.

CVE ID: **CVE-2021-22743**

CVSS v3.1 Base Score 3.9 | Low | CVSS:3.1/AV:P/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists in the Models 4351B/4352B/4355X TCM and Model 4610X UCM that could cause a module reset when the TCM receives malformed TriStation packets while the write-protect keyswitch is in the PROGRAM position.

CVE ID: **CVE-2021-22744**

CVSS v3.1 Base Score 3.9 | Low | CVSS:3.1/AV:P/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists in the Model 3009/3009X MP that could cause a module reset when the TCM receives malformed TriStation packets while the write-protect keyswitch is in the PROGRAM position. This CVE ID is unique from CVE-2021-22742, CVE-2021-22745, CVE-2021-22746, and CVE-2021-22747.

CVE ID: **CVE-2021-22745**

CVSS v3.1 Base Score 3.8 | Low | CVSS:3.1/AV:P/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists in the Model 3009/3009X MP that could cause a module reset when the TCM receives malformed TriStation packets while the write-protect keyswitch is in the PROGRAM position. This CVE ID is unique from CVE-2021-22742, CVE-2021-22744, CVE-2021-22746, and CVE-2021-22747.

CVE ID: **CVE-2021-22746**

CVSS v3.1 Base Score 3.8 | Low | CVSS:3.1/AV:P/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists in the Model 3009/3009X MP that could cause a module reset when the TCM receives malformed TriStation packets while the write-protect keyswitch is in the PROGRAM position. This CVE ID is unique from CVE-2021-22742, CVE-2021-22744, CVE-2021-22745, and CVE-2021-22747.

CVE ID: **CVE-2021-22747**

CVSS v3.1 Base Score 3.8 | Low | CVSS:3.1/AV:P/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists in the Model 3009/3009X MP that could cause a module reset when the TCM receives malformed TriStation packets while the write-protect keyswitch is in the PROGRAM position. This CVE ID is unique from CVE-2021-22742, CVE-2021-22744, CVE-2021-22745, and CVE-2021-22746.

Remediation

Affected Product and Version	Remediation
Model 3009/3009X Main Processor module installed in Tricon or Tricon CX system versions 11.3.x, 11.4.x, 11.5.x, or 11.7.x	• Call Customer Support to schedule maintenance. Schneider Electric customer engineers will have the remediated version, **Build 753 – Tricon/Tricon CX v11.8.0**, required to upgrade the module. • Module will need to be flashed with new firmware and then reinstalled in the system.

TCM Models 4351B, 4352B, and 4355X, and UCM Model 4610X installed in Tricon or Tricon CX system versions 11.3.x, 11.4.x, 11.5.0, or 11.7.0	• Call Customer Support to schedule maintenance. Schneider Electric customer engineers will have the remediated version, **Build 638 – Tricon/Tricon CX v11.5.1/v11.7.1**, required to upgrade the module. • Module will need to be flashed with new firmware and then reinstalled in the system. Later Tricon and Tricon CX system versions already incorporate this remediated version.

We strongly recommend that you use backups and evaluate the impact of these patches in a Test and Development environment or in an offline infrastructure prior to installing them in an online system. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If you choose not to apply the remediation provided above, you should immediately apply the following mitigations to reduce the risk of exploit:

- Configure the firewall to restrict network access to authorized clients as applicable.
- Apply hardening guidelines as recommended in the Triconex System Security Reference Guide (Global Customer Support account required for access).
- Disconnect TriStation 1131 from the network when not in use.
- Ensure the write-protect keyswitch is in the RUN or REMOTE state unless the system is being actively reprogrammed.
- Operator stations should be configured to display an alarm whenever the keyswitch is in the “PROGRAM” mode.

General Security Recommendations

We strongly recommend the following cybersecurity industry best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can 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.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the internet.

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information, refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2021-22742 CVE-2021-22743 CVE-2021-22744 CVE-2021-22745 CVE-2021-22746 CVE-2021-22747	• CNCERT/CC: 张嘉玮(ZHANG, Jiawei), 彭广明(PENG, Guanming)， 刘健飞(LIU, Jianfei), 张晓明(ZHANG, Xiaoming) • 昆仑数智 (Kunlun Digital Technology Co.,Ltd）： 滕征岑(TENG, Zhengcen), 吴强(WU, Qiang), 秦玉龙(Qin, Yulong)

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric products, visit the company's cybersecurity support portal page: https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH

DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *11 May 2021*	Original Release
Version 1.1 *13 July 2021*	Improved additional mitigations related to the write-protect keyswitch and clarified affected modules. (page 3)

Product Security Office Digitally signed by Product Security Office
Date: 2021.07.11 16:37:30 -04'00'