Schneider Electric Security Notification

Security Notification – EcoStruxure Triconex Tricon V3

14 December 2017 Updated 14 December 2018

Overview

In December 2018, Schneider Electric issued a security notification related to a directed incident that affected a single customer's Triconex Tricon safety shutdown system.

Schneider Electric has worked closely with the customer, independent cybersecurity organizations and the U.S. Department of Homeland Security/ICS-CERT to investigate and mitigate the risks of this type of attack. It is important to note that the legacy Tricon system responded appropriately, taking the plant to a safe state as designed. No harm was incurred by the customer or the environment.

During our extensive investigation, Schneider Electric identified a vulnerability in the Tricon firmware, which is limited to a small number of older versions of the Tricon. This vulnerability was a part of a complex malware infection scenario. To date, the information gathered indicates that if the Tricon key switch had been left in the correct position per our recommended guidelines, the injection of malware would not have been successful.

Through the recently enhanced Tricon CX controller, version 11.4, Schneider Electric has mitigated the risks of these type of malware incidents. The company has also released a process to detect the malware's presence in a Tricon controller and a procedure to remove the malware if discovered. As of February 1, 2019, Schneider Electric will require customers to have a support contract in place to engage with this malware analysis service. For more information, please contact your Global Customer Support Representative.

Schneider Electric continues to recommend customers always implement the instructions contained in the "Security Considerations" section in the Triconex documentation (i.e., Planning and Installation Guides and TriStation 1131 Developers Guide).

Affected Product(s)

- Tricon Model MP3008, versions 10.0 – 10.4

Remediation

Schneider Electric strongly recommends users upgrade to the latest Triconex Tricon CX version. Released in October 2018, Tricon CX v11.4 is compliant with the IEC 62443 cybersecurity standard and includes multiple security enhancements that meet the challenges posed by the Triton/Hatman malware techniques and other sophisticated methods of attack.

Vulnerability Details

The malware requires unrestricted access to the safety network via remote network or physical access. Additionally, the malware requires the Tricon key switch to be in the "PROGRAM" mode to successfully deploy its payload.

The malware has the capability to scan and map the industrial control system to provide reconnaissance and issue commands to Tricon controllers. Once deployed, this type of malware, known as a Remotely Accessible Trojan (RAT), controls a system via a remote network connection as if by physical access.

Detection and Mitigation

Triconex customers should contact their local Schneider Electric office for assistance with a procedure Schneider Electric has developed to detect the Hatman/Triton malware's presence in a Tricon controller and to remove the malware if discovered. Schneider Electric will fully assess the security of each Tricon safety system installation, analyze for the presence of the malware and remove it if necessary. For customers who prefer to do this on their own, Schneider Electric has made the malware detection process instructions and support material available for download via the Schneider Electric Process Automation customer support portal. Once the analysis is complete, Triconex users will receive a report for each Tricon system analyzed advising whether the malware was detected and the steps to take to remove it.

As of February 1, 2019, Schneider Electric will require customers to have a support contract in place to engage this malware detection, analysis and removal service. For more information, please contact your Global Customer Support Representative

Additionally, Schneider Electric recommends customers always keep their antivirus tools up to date and ensure they are using the latest antivirus .dat files on the engineering workstation where the TriStation terminal is installed. Signatures for the malware have been distributed to cybersecurity organizations. Schneider Electric has confirmed that major antivirus vendors now include the malware file's signatures and that if detected, the antivirus tool takes action.

Schneider Electric understands that all customers are not in a position for immediate upgrade to our latest Tricon product with our latest security features. Because of this, Schneider Electric continues to recommend customers always implement the instructions in the "Security

Considerations" section in the standard Triconex documentation (i.e., Planning and Installation Guides and TriStation 1131 Developers Guide), which include the following:

- Ensure the cybersecurity features in Triconex solutions are always enabled.
- Safety systems must always be deployed on isolated networks.
- Physical controls should be in place so that no unauthorized person would have access to the safety controllers, peripheral safety equipment or the safety network.
- All controllers should reside in locked cabinets and never be left in the "PROGRAM" mode.
- All Tristation engineering workstations should be secured and never be connected to any network other than the safety network.
- All methods of mobile data exchange with the isolated safety network such as CDs, USB drives, DVD's, etc. should be scanned before use in the Tristation engineering workstations or any node connected to this network.
- Laptops and PCs should always be properly verified to be virus and malware free before connection to the safety network or any Triconex controller.
- Operator stations should be configured to display an alarm whenever the Tricon key switch is in the "PROGRAM" mode.

Cyber Preparedness:

- Also, review and assess your site's cyber preparedness. Schneider Electric is a proponent of the NIST Cyber Security 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.
- If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: http://www.schneider-electric.com/b2b/en/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp%20

For More Information

- ICS-CERT - https://ics-cert.us-cert.gov/advisories

If you have any questions, please contact your local Service Representative or a Schneider Electric Support Center at:

GCS Center	America's GCS	Asia Pacific GCS	EMEA GCS
Location	Foxboro MA USA	Shanghai	Baarn NL
Phone	+1-866-746-6477	+86 21 37180086	+31-3554-84125
Internationally	+1-508-549-2424		

Fax	+1-508-549-4999	+86 21 37180196	+31-3554-84230
Email	America's GCS	Asia Pacific GCS	EMEA GCS

To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

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

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS, AND IS PROVIDED ON AN "AS-IS" BASIS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 13 December 2017	Original Release
Version 1.1 14 December 2017	- Updated targeting to affected in title and first sentence.
Version 2 18 January 2018	- Updated Details, Detection and Mitigation Sections
Version 3 14 December 2018	- Updated reflecting availability of Tricon CX v11.4 and that detection and removal tool and procedure becomes available only through a customer service agreement effective January 1, 2019.

Product Security Office

Digitally signed by Product Security Office
Date: 2018.12.14 10:56:19 -05'00'