

## Important Security Notification

---

### Malware Discovered Affecting Triconex Safety Controllers V1.1

December 14, 2017

#### Overview

---

Schneider Electric is aware of a directed incident affecting a single customer's Triconex Tricon safety shutdown system.

---

We are working closely with our customer, independent cybersecurity organizations and ICS-CERT to investigate and mitigate the risks of this type of attack. While evidence suggests this was an isolated incident and not due to a vulnerability in the Triconex system or its program code, we continue to investigate whether there are additional attack vectors. It is important to note that in this instance, the Triconex system responded appropriately, safely shutting down plant operations. No harm was incurred by the customer or the environment.

Triconex user documentation contains detailed security guidelines and recommendations on how to protect Triconex systems from attack. We strongly encourage all our customers to follow these recommendations regarding product use and security, as well as apply and follow industry-recognized cybersecurity best practices at all times to protect their installations:

- Ensure the cybersecurity features in Triconex solutions are always enabled;
- Never leave the front panel key position in the "Program" mode when not actively configuring the controller;
- And ensure all TriStation terminals, safety controllers and the safety network are isolated from the rest of the plant communication channels.

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 should this be necessary.

The Schneider Electric Product Security Office continues to work with ICS-CERT and will update this advisory as more information becomes available.

#### Details

The modules of this malware are designed to disrupt Triconex safety controllers, which are used widely in critical infrastructure. The malware requires the keyswitch to be in the "PROGRAM" mode in order to deliver its payload. Among others, the reported malware has the capability to scan and map the industrial control system environment to provide reconnaissance and issue commands directly to Tricon safety controllers.

## Important Security Notification

### Detection and Mitigation

Signatures for this malware in its current form have been distributed to cybersecurity organizations. Please see below for additional information.

Schneider Electric recommends customers follow the instructions contained in the “Security Considerations” section within the [Planning and Installation Guide](#) for each respective Triconex controller (Tricon, Trident, Tri-GP), which include the following:

- Safety systems must always be deployed on isolated networks using zones and conduits as defined in IEC-62443;
- Physical controls should be in place so no unauthorized person has access to the plant, equipment rooms, safety controllers, safety peripheral equipment or the safety network;
- All controllers should reside in locked cabinets and never be left in the “Program” mode;
- All TriStation terminals (Triconex programming software) should be kept in locked cabinets and should 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, etc., should be scanned before use in the TriStation terminals or any node connected to this network;
- Laptops that are connected to any other network-- beside the safety network-- should never be allowed to connect to the safety network without proper sanitation;
- Operator stations should be configured to display an alarm whenever the Tricon keyswitch is in the “Program Mode”; key removed and secured;
- Enhanced security features in TriStation, as well as the Triconex communication modules, should be enabled.

For a comprehensive list of Triconex security recommendations, please refer to the user documentation 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>

### For More Information

- FireEye:
  - <https://www.fireeye.com/>
- Dragos Cybersecurity:
  - <https://dragos.com/>

## Important Security Notification

---

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

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. 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>

### 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](http://www.schneider-electric.com)

<b>Version 1</b> <i>13 December 2017</i>	Original Release
<b>Version 1.1</b> <i>14 December 2017</i>	Updated <b>targeting</b> to <b>affected</b> in title and first sentence.