Life Is On Schneider Electric

Schneider Electric Security Notification

ConneXium Gateway TSXETG100 and PowerLogic Ethernet Gateway EGX100 (V2)

14 May 2019 (12 November 2019)

Overview

Schneider Electric is aware of a vulnerability in its ConneXium Gateway TSXETG100 and PowerLogic Ethernet Gateway EGX100 products.

Affected Product(s)

TSXETG100

EGX100 – all variants

- EGX100SD
- EGX100MG
- EGX100SQD
- EGX100SDR
- EGX100M
- EGX100MGAA
- EGX100MGBA
- EGX100MGBB
- EGX100MGBC

ECI850 – all variants

- ECI850
- ECI850MG

Vulnerability Details

CVE ID: **CVE-2018-7834**

CVSS v3.0 Base Score 6.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

A CWE-79 Cross-Site Scripting vulnerability exists allowing an attacker to send a specially crafted URL with an embedded script to a user that would then be executed within the context of that user.

Remediation

Schneider Electric's ConneXium TSXETG100 and PowerLogic EGX100 Gateways have reached end of life and are no longer commercially available as of December 31st, 2016. The

Schneider Electric Security Notification

EGX150 (Ethernet Gateway Link 150) offer is available to replace this product. Customers should strongly consider upgrading to EGX150.

Customers should immediately apply the following workarounds and mitigations to reduce risks while still using the TSXETG100 and EGX100:

- Use of an application firewall to check the user's inputs and block the traffic accordingly

or

- Use a standard firewall to limit the HTTP traffic on your network and restrict the unauthorized access to the TSXETG100 and EGX100 products.

Product Information

TSXETG100 and EGX100 are Ethernet Gateways used to convert Modbus TCP to Modbus serial protocols.

Product Category - Industrial Automation Control

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

Product Category - Building and Automaiton Control

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

TSXETG100 and EGX100 Gateways – any version

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.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the "Program" mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.

- Minimize network exposure for all control system devices and/or 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), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2018-7834	Ezequiel Fernandez

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 and/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

Schneider Electric Security Notification

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *14 May 2019*	Original Release
Version 2 *12-Nov-19*	Updated affected products to include *EGX100* and *ECI850* variants (page 1)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.11.08 13:09:43 -05'00'