Vulnerability Disclosure – ETG3000 FactoryCast HMI Gateway

8-Jan-2015

Overview

Schneider Electric has become aware of vulnerabilities in the ETG3000 FactoryCast HMI product line.

Vulnerability Overview

The vulnerabilities identified include:

- Unauthenticated access to configuration data using XMLRPC interface
- Unauthenticated access to JAR file
- FTP account

Product(s) Affected

The products affected include:

- TSXETG3000 all versions
- TSXETG3010 all versions
- TSXETG3021 all versions
- TSXETG3022 all versions

Vulnerability Details

- Unauthenticated access to configuration data using XMLRPC interface. XMLRPC interface of device allows unauthenticated access to device configuration.
- Unauthenticated access to JAR file. It is possible to access rde.jar file without any authentication.
- Device is accessible over FTP using hard-coded credentials.

Mitigation

Item 1 – Unauthenticated access to configuration data using XMLRPC interface
Schneider Electric recommends user to change the default login credentials (USER / USER). Doing so, configuration files will be protected against unauthorized access

Item 2 & 3 - Unauthenticated access to JAR file & FTP account
Schneider Electric has produced a patch, labelled V1.60 IR 04. . With this new release, the jar files directory have been placed in a secure area, and the FTP server can be deactivated when not needed.

This new firmware release is available on our web site. Click here:

Schneider Electric wishes to acknowledge and thank Qualys for their findings and support to resolve these vulnerabilities.

For More Information

This document is intended to help provide an overview of the identified vulnerability 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 on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com