InTouch Machine Edition 2014 Vulnerabilities

23-Feb-2015

Overview

Schneider Electric has become aware of vulnerabilities in the InTouch Machine Edition 2014 product line.

Vulnerability Overview

The vulnerabilities identified include:

- Sensitive Information Protected with Hard-coded Keys
- User Enumeration
- Unencrypted User Credentials
- Cleartext OPC password storage

Product(s) Affected

The product(s) or product lines affected include:

- InTouch Machine Edition 2014, version 7.1.3.2 and all previous versions

Vulnerability Details

- Sensitive information is stored in Project Files and Project Configuration Files. This information is protected using a hard-coded, clear text password.
  - CVSS 4.7 (AV:L/AC:M/Au:N/C:C/I:N/A:N)
- When connecting to server from HMI, available user names are presented to the screen allowing for potential brute force attacks
  - CVSS 3.3 (AV:A/AC:L/Au:N/C:P/I:N/A:N)
- User credentials are sent in clear text allowing for malicious actors to access the control system
  - CVSS 3.3 (AV:A/AC:L/Au:N/C:P/I:N/A:N)
- OPC User Credentials are stored in a configuration file in cleartext

- CVSS 5.2 (AV:L/AC:L/Au:S/C:C/I:P/A:N)

Schneider Electric would like to thank Gleb Gritsai, Alisa Esage Shevchenko, and team from Positive Technologies for their discovery and cooperation during this vulnerability disclosure process.

Mitigation

Schneider Electric has released patches, available for download, to remediate the noted vulnerabilities.

The patch for InTouch Machine Edition 2014, Version 7.1.3.4, Service Pack 3, Patch 4, is available for download using this URL (registration required):

https://gcsresource.invensys.com/tracking/ConfirmDownload.aspx?id=21276

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