ICS-CERT ADVISORY

ICSA-11-231-01—INDUCTIVE AUTOMATION IGNITION INFORMATION DISCLOSURE VULNERABILITY

August 19, 2011

OVERVIEW

ICS-CERT has received a report from Rubén Santamarta concerning a vulnerability in Inductive Automation's Ignition software. Ignition is an updated version of FactoryPMI (Plant Management Interface), offered by Inductive Automation. This vulnerability allows unauthorized users to download files containing important information about the system and project.

ICS-CERT has worked with Inductive Automation and Rubén Santamarta to confirm this vulnerability, and Inductive Automation has issued a patch to address it. ICS-CERT has validated that this patch fully resolves this vulnerability.

AFFECTED PRODUCTS

Inductive Automation Ignition versions prior to Version 7.2.8.178 are affected.

IMPACT

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Ignition is an updated version of FactoryPMI, offered by Inductive Automation. Ignition is a full featured human-machine interface/SCADA product used in a variety of industrial applications that is produced by Inductive Automation. According to Inductive Automation, Ignition has known deployments in North and South America, Europe, Australia, and across Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

According to the researcher's report, the vulnerability is exploitable by connecting a specific Uniform Resource Locator (URL) address. The successful connection to this URL results in a prompt to download files containing important details about system and project information, including authorized usernames and password hashes.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

Exploiting this vulnerability requires a low skill set.

MITIGATION

Inductive Automation has produced Version 7.2.8 of the affected software available on the Inductive Automation Downloads website (http://www.inductiveautomation.com/downloads). Customers who are unfamiliar with the Inductive Automation upgrade routine should contact the vendor for assistance.

According to its website, Inductive Automation Support can be reached at (916) 456-1045 or support@inductiveautomation.com.

ICS-CERT encourages asset owners to minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Locate control system networks and remote devices behind firewalls and isolate them from the business network. When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) provides a section for control system security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[a]

a. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.