Rockwell Automation Product Security Incident Response Framework

Rockwell Automation issues the following summary of its product security incident response program to support its customers with their incident response planning and any other related activities, such as a "tabletop exercises." Rockwell Automation understands the increasing necessity of cybersecurity in industrial control systems (ICS), as well as supporting its customers and partners in their security initiatives. This includes those instances where a Rockwell Automation product, solution, or service could potentially be involved in a security incident. For clarity Rockwell Automation uses the term "incident" as "the act of violating an explicit or implied security policy" as defined by the NIST Special Publication 800-61, Computer Security Incident Handling Guide.

The Rockwell Automation Incident Response Framework is comprised of the following phases: 1) Notification, 2) Assessment & Containment, and 3) Remediation, Incident Post-Mortem, and Improvement Plan. This framework supports customers and partners in instances where they may be potentially affected by a cybersecurity incident or breach.

Notification

The affected party should contact the Rockwell Automation Product Security Incident Response Team (RA PSIRT) via email at secure@ra.rockwell.com with a brief description of the product security incident within their environment. The affected party should provide contact information for responsible personnel from their organization(s). Details related to the security incident, including without limitation the observed Confidentiality-Integrity-Availability (CIA) impact and the Rockwell Automation product(s) believed to have been compromised, will help the RA PSIRT to begin efforts with the relevant internal stakeholders when scheduling the initial Incident Response Coordination Call within 24 hours of reporting.

Assessment & Containment

The Incident Response Coordination Call serves to assess and assign the priority of response which aids in determining the relevant response actions. Priority is determined by the RA PSIRT using industry standards, which include but are not limited to, the following: potential safety and regulatory concerns, loss of product or system availability, loss of integrity or confidentiality of data, and extent of impact ranging from a local to global standpoint. Post-assessment and an agreed upon Incident Action Plan will be developed that outlines actions and goals to be accomplished during the first operational response period. Following containment, both parties shall follow their internal security policies and procedures for preservation of evidence to aid in analysis of the event and remediation, with RA PSIRT providing support when needed.

Remediation, Incident Post-Mortem, & Improvement Plan

Until the incident is remediated, RA PSIRT will coordinate additional calls with the affected party and regional persons of contact (POCs) every six to 24 hours for status updates. Successful implementation of a remediation strategy is followed by an Incident Post-Mortem. Any security vulnerability in a Rockwell Automation product during the Incident Post-Mortem will trigger the ISO/IEC 29147 and 30111 aligned vulnerability response processes to assess, remediate, and responsibly disclose the issue. Additionally, Rockwell Automation provides services for long-term remediation options to identify, protect, and recover from security incidents. The post-mortem shall determine successful actions, as well as areas for improvement between the organizations' response procedures through an established Improvement Plan.

This document is solely intended to be used as a high-level overview of the response framework. All information in this document is provided "As Is". Rockwell Automation may make changes to the framework and this document at any time in its sole discretion without notice. If you have any follow up questions, please contact Rockwell Automation PSIRT via email at secure@ra.rockwell.com

Publication RA-WP004A-EN-P — March 2020