PRODUCT SECURITY VULNERABILITIES

Frequently Asked Questions

Allen-Bradley

LISTEN. THINK. SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

PRODUCT SECURITY VULNERABILITIES

Frequently Asked Questions

Allen-Bradley

Vulnerabilities

WHAT IS A VULNERABILITY?

A vulnerability is a flaw or weakness in a product or system that can be exploited to compromise the product or system's confidentiality, integrity, and/or availability.

WHAT IS CYBERSECURITY? WHY IS IT IMPORTANT?

Cybersecurity is the collection of technologies, processes and practices that help protect networked computer systems from unauthorized use or harm. Broadly speaking cybersecurity topics can be subdivided into cyber-attacks, which are offensive in nature and emphasize network penetration techniques, as well as cyber-defenses, which are defensive in nature and emphasize counter-measures intended to help eliminate or mitigate cyber-attacks.

The main goals of cybersecurity in an industrial setting are simple:

1. *Availability: maintain and never give up control in a control system;*
2. *Confidentiality: keep proprietary information IN and that only individuals with a need-to-know have access to the information; and*
3. *Integrity: ensure that the information flowing through the system has not been tampered with.*

Industry-standard Systems

WHAT IS ICS-CERT?

The United States' Department of Homeland Security ("DHS") includes the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"), whose mission is to guide the security efforts between government and industry to improve the cyber security posture of control systems within the nation's critical infrastructure. ICS-CERT assists control systems vendors, as well as asset owners and operators, to identify security vulnerabilities and develop sound mitigation strategies that strengthen their cyber security posture and reduce risk. For more information you can go to https://ics-cert.us-cert.gov/.

ICS-CERT maintains several information portals for disseminating security information to owners and operators of Industrial Control Systems:

1. *Alerts: Timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks*
2. *Advisories: Timely information about current security issues, vulnerabilities, and exploits.*
3. *Secure Portal: Owners/operators of U.S. critical infrastructure can apply for membership in the Secure Portal, to receive early notification of security issues, vulnerabilities, and exploits.*
4. *ICS-CERT Monitor Newsletters: Periodic publication of security news and information applicable to Industrial Control System owners/operators.*

WHAT DOES CVSS MEAN?

The Common Vulnerability Scoring System ("CVSS") is a free and open industry standard for assessing the severity of computer system security vulnerabilities. It is widely used by industrial control systems vendors like Rockwell Automation. CVSS-based scores are included in each Product Security Advisory and help customers assess their risk and exposure (including how to prioritize their responses and resources according to a specific threat). For more information you can go to https://www.first.org/cvss/specification-document.

WHAT IS A LAYERED SECURITY MODEL AND DEFENSE IN DEPTH?

Layered security and defense in depth are the practice of combining multiple mitigating security controls to help protect systems, resources and data. The term is based on a military strategy involving multiple layers of defense that may or may not resist rapid penetration by an attacker but may exhaust the attacker since. In the cybersecurity world these terms assume more than just technical security tools deployment; they also imply implementing cybersecurity policies that include operations planning, user training, and physical access security measures.

The Rockwell Automation Strategy for Product Security Vulnerabilities

WHAT IS ROCKWELL AUTOMATION DOING TO MAKE ITS PRODUCTS MORE SECURE?

Rockwell Automation recognizes the importance of security in industrial control systems and is investing in its products, people, industry-leading partnerships, and our integrated consulting services (Networks & Security Services – NSS) to enhance the security in our products while maintaining productivity.

One example of our partnership activities, in conjunction with Cisco, is that Rockwell Automation published the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, a validated reference architecture that provides explicit defense in depth measures and design practices to enhance system and device level security. Our newer generations of products include hardening features such as software/firmware digital signing, firmware encryption, hardware-based cryptographic key storage, and network resiliency testing. Rockwell Automation collaborates with appropriate government agencies, and is also active in standards bodies such as ISA/IEC-62443. Lastly, we listen to the concerns of our customers, and address security concerns related to our offerings.

DOES ROCKWELL AUTOMATION HAVE A PROCESS TO DEAL WITH POTENTIAL SECURITY VULNERABILITIES IN ROCKWELL AUTOMATION/ALLEN-BRADLEY/ROCKWELL SOFTWARE PRODUCTS?

Yes. The Rockwell Automation Security Vulnerability Process is based on ISO29147 and ISO30111, which define standards for receiving and processing vulnerability reports. Product security concerns that are received via secure@ra.rockwell.com are immediately routed to the Rockwell Automation Product Security Incident Response Team ("PSIRT") dedicated to supporting the needs of our customers and government institutions. The PSIRT reviews the claims to evaluate validity, reproducibility and scope of impact using CVSS. The PSIRT then determines what – if any — risk mitigation is required. Lastly, the PSIRT communicates vulnerabilities and risk mitigations through direct means and/or via other known communication channels (e.g. Rockwell Automation® Knowledgebase, Product Notifications,
ICS-CERT).

WHY ARE ROCKWELL AUTOMATION AND OTHER INDUSTRIAL CONTROL SYSTEMS AND AUTOMATION VENDORS PROVIDING DISCLOSURES AND ADVISORIES?

Rockwell Automation is committed to providing detailed and actionable information about security vulnerabilities to drive awareness and encourage customers to make informed decisions on what steps they must take to improve their security.

HOW DO I FIND A LIST OF ALL PUBLISHED ROCKWELL AUTOMATION PRODUCT VULNERABILITIES?

Visit the Rockwell Automation Security Advisory Index at: https://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102.

Customers are also encouraged to visit the Rockwell Automation public security web page at: http://www.rockwellautomation.com/security for new and relevant information relating to the security of our products.

WHAT IS THE DIFFERENCE BETWEEN A PRODUCT SECURITY ADVISORY AND A PRODUCT SAFETY ADVISORY (PSA) OR A PRODUCT NOTICE?

*A Product Safety Advisory ("PSA") is issued when a product failure may result in significant loss of capital equipment, personal injury, or death. Customer action is **REQUIRED**.*

*A Product Notice ("PN") is issued when a product failure may result in significant commercial loss or customer dissatisfaction. Customer action is **STRONGLY RECOMMENDED**.*

*A Product Security Advisory is issued for security alerts and security recommendations where such risks stem from cyber-attacks. These advisories are intended to raise customer awareness of risks to affected product operation or performance and also supply relevant recommendations for how to reduce or remove the risk associated with a vulnerability. Customer action is **STRONGLY RECOMMENDED**.*

WHERE CAN I LEARN MORE ABOUT INDUSTRIAL SECURITY AND HOW ROCKWELL AUTOMATION IS INVOLVED?

In addition to your local Rockwell Automation sales resources, you can find more security information, including links to key resources associated with industrial security at the Rockwell Automation Security Solutions web page located at http://www.rockwellautomation.com/solutions/security.

WHAT ARE THE MEANS BY WHICH ROCKWELL AUTOMATION COMMUNICATES INCIDENTS TO CUSTOMERS?

Rockwell Automation uses several methods to communicate product security information to our customers. These methods include:

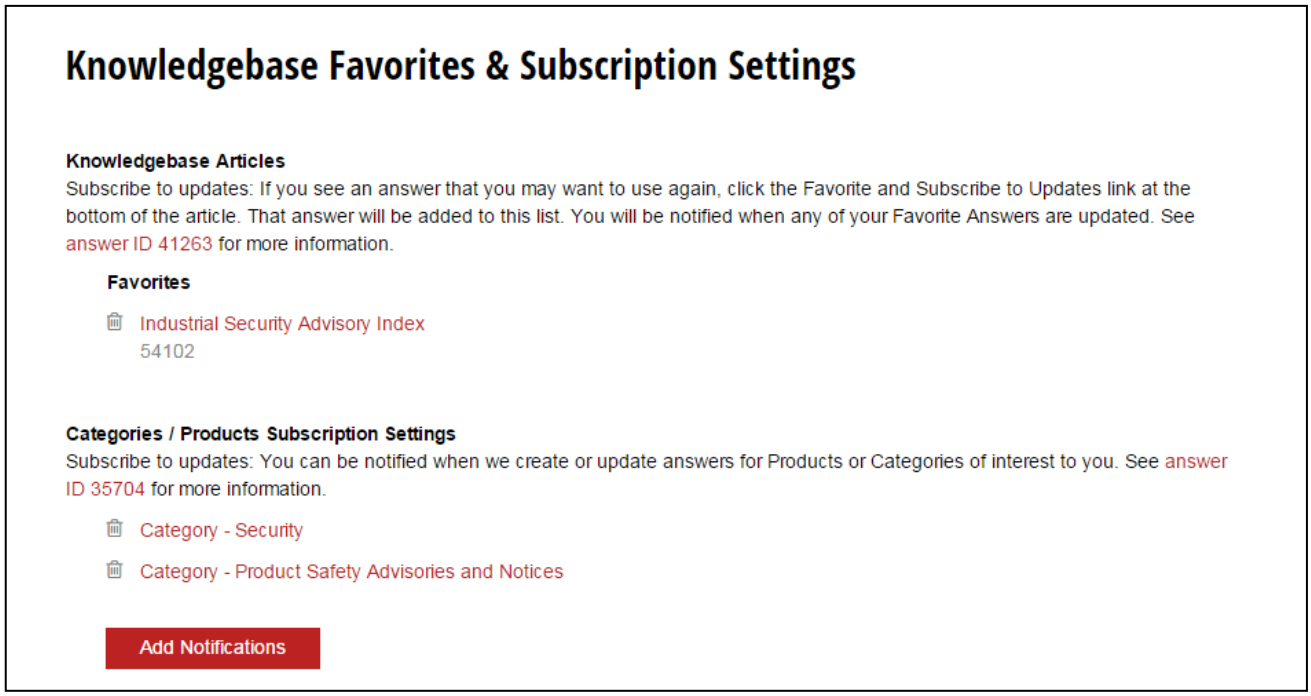
1. *Rockwell Automation Knowledgebase: Establish a free Knowledgebase account and subscribe to Knowledgebase article KB54102 entitled "Industrial Security Advisory Index". This article is a publicly available resource and subscription service that points to specific Rockwell Automation product security alerts, advisories and security recommendations.*
2. *ICS-CERT: Rockwell Automation maintains a close relationship with ICS-CERT. We coordinate the publication of product security information with ICS-CERT in order to reach as many customers as possible. Find ICS-CERT publications of Rockwell Automation vulnerabilities on the Alerts and Advisory pages.*

HOW CAN I BE AUTOMATICALLY NOTIFIED OF SECURITY INCIDENTS?

Rockwell Automation recommends that customers subscribe directly to ICS-CERT notifications through their RSS feeds, Twitter, and/or Email notifications. U.S.-based customers should register and subscribe to the ICS-CERT Secure Portal.

In Rockwell Automation Knowledgebase, by selecting "Subscribe to updates" located at the bottom of KB54102: Industrial Security Advisory Index or by selecting the "Category – Security" in your profile, you will be notified via a weekly email of any new or changed content in this article. When Rockwell Automation determines that a security article is of higher importance, an email from Knowledgebase will be sent to all customers who have selected the category of security in their profile. We strongly recommend customers set up a Knowledgebase account and subscribe to the "KB54102: Industrial Security Advisory Index".

A screenshot of how your profile page would be selected for receiving both Product Safety / Product Notices and Product Security Advisories is shown below:



HOW CAN I GET MORE HELP TO MANAGE MY SECURITY RISK?

Rockwell Automation Network & Security Services consulting services are available to assist customers with assessing and improving the state of security of industrial control systems that use Rockwell Automation and other vendor control products. Bringing you a unique blend of expertise in both the IT and industrial automation spaces, we provide you with a holistic approach to managing your network infrastructure and security throughout its lifecycle. More information is available at http://www.rockwellautomation.com/services/security and http://literature.rockwellautomation.com/idc/groups/literature/documents/pp/gmsn-pp002_-en-p.pdf.

DOES ROCKWELL AUTOMATION PROVIDE A PRODUCT SECURITY WARRANTY?

Rockwell Automation does not provide a product security warranty.

DOES ROCKWELL AUTOMATION VALIDATE MICROSOFT PATCHES SO THAT I CAN KEEP PCS AND SERVERS UP TO DATE? OTHER 3RD PARTY SYSTEMS?

Customers have asked Rockwell Automation to provide a level of assurance that a given Microsoft ("MS") security update will not hinder the functional operation of their Industrial Control Systems. In 2005 the MS Patch Qualification team ("PQUAL") was formed to qualify Microsoft security updates against the most popular set of products available from Rockwell Automation.

Microsoft regularly releases Security Updates on the second Tuesday of each month. Testing by the PQUAL team begins on Patch Tuesday and our results are published within ten business days on the Patch Qualification Portal. Security Updates released outside of cycle are known as "Out-of-Band" updates. These are typically released due to a publicly disclosed vulnerability, such as a Virus, Worm, or Trojan that will likely affect a large number of users. The PQUAL team makes every effort to handle occasional Out-of-Band patches as quickly as possible.

Customers who wish to review notifications when new results are available should visit and subscribe to updates on KB35530.

DOES ROCKWELL AUTOMATION PROVIDE PC/SERVER HARDENING GUIDANCE SO THAT I CAN FURTHER REDUCE MY RISK?

Rockwell Automation has published KB546987 which contains links to additional guidance in several key areas of PC/Server security. Customers can subscribe to updates on KB546987 to receive notifications when new resources are available.

HOW DO I REPORT A PRODUCT SECURITY VULNERABILITY TO ROCKWELL AUTOMATION?

To address specific concerns or to report issues with Rockwell Automation/Allen-Bradley/Rockwell Software products, please contact us through our secure@ra.rockwell.com email address. Vulnerability details should be encrypted with our PGP Public Key to help protect the confidentiality of the information.