REAL Matters
Protecting Your OT Assets and Infrastructure
ICSSbD Industrial Control Systems Secure by Design
Volume 1, Advisory #7 – June 2022

REAL Matters advisories are published to communicate cybersecurity threats and risks within the Operational Technology (OT) environment and where Critical Infrastructure vulnerabilities are identified. The purpose of this newsletter is to inform, propose suggested approaches to mitigate the risk as well as provide feedback on how Mangan Cybersecurity is approaching the issue(s) addressed.

Advisory Information

At A Glance

Issue Date:	June 1, 2022
Summary:	Rockwell Automation reports a Class 3 Common Industrial Protocol message vulnerability which will result in an unrecoverable major fault. This fault will require a user project file redownload to the controller.
Systems Impacted:	CompactLogix 5380, Compact GuardLogix 5380, CompactLogix 5480, CompactLogix 5370 and Compact GuardLogix 5370 controllers: firmware Versions 33.013 and earlier ControlLogix 5580 and ControlLogix 5570 controllers: firmware Versions 33.013 and earlier GuardLogix 5570 and GuardLogix 5580 controllers: firmware Versions 32.013 and earlier
Importance:	Moderate

Details

A malformed Class 3 CIP message configured for cached connection may cause a denial-of-service attack. A Class 3 CIP message is a controller message requiring a response and is typically designed with the MSG instruction. An adversary might access the controller to exploit the vulnerability by sending the malicious message to another device in the control architecture.

Actions and/or Recommendations

Upgrade to and design projects using the latest firmware - CompactLogix 5380, Compact GuardLogix 5380, CompactLogix 5480, ControlLogix 5580, GuardLogix 5580: Upgrade to v33.011 firmware

CompactLogix 5370, Compact GuardLogix 5370, ControlLogix 5570, GuardLogix 5570: Upgrade to v34.011 firmware.

If immediate upgrades are not possible then make use of Microsoft AppLocker or other similar allow-listing to protect against exploits. Assure workstation and server least-privilege user and service accounts. Understand that adversary attacks can take place through these vulnerable computers.

Additionally, follow Rockwell Automation recommendations for using trusted software, deploying patches and antivirus and antimalware software. Minimize the attack surface of the control network perimeter. Secure data flow from the control zones to the business environment.

If remote access is required, use secure methods, such as VPNs be aware that VPNs may have vulnerabilities which require updates and patches.

About Mangan Inc.

Mangan Inc. is a nationally-recognized Specialty Engineering, Automation, and Integration company, providing a full-range of services to the Oil & Gas, Refining, Pipeline, Chemicals, and Life Sciences Industries. Established in Long Beach, California in 1990, Mangan's multiple office locations include sites in California, Georgia, New Hampshire, North Carolina, Texas, and Louisiana. Mangan's 350+ employee-owners bring expertise, innovation, and safety as their core mission to some of the largest companies in the world.