EMERSON CYBERSECURITY NOTIFICATION

ID number and revision	EMR.RMT20004, revision 3
Date	25 January 2021
Affected Product:	Rosemount Transmitter Interface Software (all versions) SKUs: • 04088-9000-0001 • 04088-9000-0002 • 7000003-312
CVE	https://nvd.nist.gov/vuln/detail/CVE-2020-12525
CVSSv3.1 Base Score	7.3* (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C) *Score provided by the 3rd party that notified Emerson of this issue

Security is an important part of the success of your business. Emerson maintains dedicated security staff to continuously monitor and analyze potential security issues. We also engage third party experts to help us design and maintain robust security features within our products. We are committed to reviewing threats as they become known, issuing notifications when necessary, and providing mitigations and solutions in a timely manner. If you transferred any of the affected products in question, please immediately forward this important Cybersecurity Notification to the eventual user so they can take appropriate action.

Executive Summary

Emerson was recently made aware of a vulnerability in the application known as *Rosemount Transmitter Interface Software (RTIS)* by the contracted developer of the application, M&M Software (https://www.mm-software.com). RTIS is primarily used with the Rosemount model 4088.

In coordination with M&M Software, the vulnerability has been publicly disclosed through the United States Cybersecurity & Infrastructure Security Agency (CISA) on January 21st. More details on the root vulnerability from M&M can be found on the CISA website (https://us-cert.cisa.gov/ics/advisories/icsa-21-021-05) and through VDE CERT (https://cert.vde.com/en-us/advisories/vde-2020-048).

Risk Assessment

Based on the vulnerability information provided by M&M Software, a malicious user with write access to the file system of the engineering station where RTIS is installed could potentially modify data intended for use by RTIS (i.e. a project file). If that data is modified maliciously, it could then potentially be executed by RTIS (at RTIS's privilege level) when that maliciously modified project file is loaded.

Recommendations

Emerson recommends users ensure all workstations used to interact with field instruments be protected using industry standards (e.g. ISA/IEC 62443) and your company's security policies and procedures. Furthermore, Emerson has made the decision to discontinue RTIS and no additional software updates will be provided. Therefore, Emerson recommends users transition to the free *AMS Instrument Inspector* software as a replacement device configuration tool. More information on *AMS Instrument Inspector* including directions on how to download this software, can be found at: https://www.emerson.com/en-us/catalog/ams-instrument-inspector.

© Emerson

Legal Disclaimer

The urgency and severity ratings of this notification are not tailored to individual users; users may value notifications differently based upon their system or network configurations and circumstances. THIS NOTIFICATION, AND INFORMATION CONTAINED HEREIN, IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. THE USE OF THIS NOTIFICATION, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THIS NOTIFICATION, IS AT YOUR OWN RISK. EMERSON RESERVES THE RIGHT TO CHANGE OR UPDATE NOTIFICATIONS AT ANY TIME.

Emerson Cyber Security Notification Categories

	Alert	Alerts are issues that could have immediate, direct, and serious impact on Emerson systems. Alerts require immediate action to mitigate the risk and prevent disruption to operation. Software and firmware updates should be performed as soon as possible.
	Advisory	Advisories are issues that have the potential to be exploited against an Emerson system. The only action typically required would be the verification that the Emerson system is well protected and configured as recommended. Firmware updates should be performed at next convenient opportunity.
	Informational	Informational bulletins provide clarification on issues that cannot be used as an exploit against an Emerson system.

Contact Information

Please contact your local Rosemount/Emerson Automation Solutions sales representative or Rosemount directly, with any questions regarding this issue or for technical support. For additional assistance, please contact Rosemount by any of the methods below.

1. **Emerson Global Customer Care (24/7 Support)**

   Phone: +1 888 889 9170
   Email: ContactUs@Emerson.com

2. **Rosemount North American Response Center (24/7 Support – includes Canada)**

   Phone: +1 800 654 7768

3. **Email to Rosemount Quality Feedback**

   RMT-NA.SpecialistDPFlow@emerson.com

© Emerson