

EMERSON CYBER SECURITY NOTIFICATION

ID number and revision	EMR.RMT21003, revision 2
Date	17-December-2021
Products:	
<ul style="list-style-type: none"> • <i>Emerson Plantweb Insight</i> • <i>Emerson Wireless Gateways (all versions)</i> • <i>Emerson WirelessHART Instruments</i> • <i>Rosemount Wireless Permasense Products</i> • <i>Permasense Data Manager Suite</i> • <i>Emerson Location Awareness Solution</i> • <i>Emerson Security Setup Utility</i> • <i>Paine Branded Digital Products</i> • <i>Rosemount Nuclear Products</i> • <i>700 & 800 Core Processor</i> • <i>820 Coriolis Transmitter</i> • <i>1500, 1600, 1700 Transmitter</i> • <i>2400S, 4200, 5700 Series Coriolis Transmitter</i> • <i>2500, 2700, 3300, 3350, 3500, 3700, 4700 Transmitters</i> • <i>9739 MVD Coriolis Transmitter</i> • <i>FMT & LFT Coriolis Transmitter</i> • <i>GDM, SGM, CDM Transmitters</i> • <i>K-Series Coriolis Transmitters</i> • <i>Prolink Configuration Software</i> • <i>Prolink Mobile Application & ProcessViz Software</i> • <i>4732 Endeavor</i> • <i>Vortex and Magmeter Transmitters</i> • <i>USM 3410 and 3810 Series Ultrasonic Transmitters</i> • <i>Mark III Gas and Liquid USM</i> • <i>Flarecheck, FlowCheck, Flowel & PWAM software</i> • <i>MPFM2600 & MPFM5726</i> • <i>DHNC1, DHNC2</i> • <i>WCM, SWGM</i> • <i>Fieldwatch and Service consoles</i> • <i>5726 Transmitter</i> • <i>Plantweb Advisor for Metrology and Metering Suite SDK</i> • <i>Gas Chromatographs: M500/2350A, MON2000, 700XA/1500XA, 370XA, MON2020</i> • <i>Gas Analysis: X-STREAM Enhanced (XEGP, XEGK, XEGC, XEGF, XEFD, XECLD)</i> • <i>Gas Detection: Millennium II Basic, Single & Dual Channel, 928 Wireless Gas Monitor/628 Gas Sensor, 935 & 936 Open Path Gas Detector, Millennium Air Particle Monitor</i> • <i>Incus Ultrasonic gas leak detector</i> • <i>Flame Detection: 975UF & 975UR Infrared Flame Detectors, 975HR Infrared Hydrogen Flame Detector, 975MR Multi-Spectrum Infrared Flame Detector</i> • <i>Liquid Transmitters: 5081, 1066, 1056, 1057, 56</i> • <i>Combustion: OCX, OXT, 6888, CX1100, 6888Xi</i> • <i>Spectrex family Flame Detectors and Rosemount 975 flame detector</i> • <i>CT4400 – QCL General Purpose Continuous Gas Analyzer</i> 	

- *CT5400 – QCL General Purpose Continuous Gas Analyzer*
- *CT5100 – QCL Field Housing Continuous Gas Analyzer*
- *CT5800 – QCL Flameproof Housing Continuous Gas Analyzer*
- *CT4215 – QCL Packaging Leak Detection System*
- *CT2211 – QCL Aerosol Microleak Detection System*
- *CT4404 – QCL pMDI Leak Detection Analyzer*
- *CT4000 – QCL Marine OEM Gas Analyzer*
- *CT3000 – QCL Automotive OEM Gas Analyzer*
- *3051 & 3051S Pressure transmitter families*
- *2051 Pressure Transmitter Family*
- *4088 Pressure Transmitter*
- *2088 Pressure Transmitter Family*
- *2090F/2090P Pressure Transmitters*
- *4600 Pressure Transmitter*
- *215 Pressure Sensor Module*
- *550 PT Pressure Transmitter*
- *326P Pressure Transmitter*
- *3144P Temperature Transmitter*
- *644 Temperature Transmitter*
- *848T Temperature Transmitter*
- *148 Temperature Transmitter*
- *248 Temperature Transmitter*
- *326T Temperature Transmitter*
- *327T Temperature Transmitter*
- *648 Temperature Transmitter*
- *4088 Upgrade Utility*
- *Engineering Assistant 5.x & 6.x*
- *248 Configuration Application*
- *Rosemount IO-Link Assistant*
- *Rosemount TankMaster and TankMaster Mobile*
- *Rosemount RadarMaster and RadarMaster Plus*
- *Rosemount Radar Configuration Tool*
- *Rosemount 2460 System Hub*
- *Rosemount 2410 Tank Hub*
- *Rosemount 3490 Controller*
- *Rosemount 2230 Graphical Field Display*
- *Rosemount 2240S Multi-input Temperature Transmitter*
- *Rosemount CMS/SCU 51/SCC*
- *Rosemount CMS/WSU 51/SWF 51*
- *Rosemount CMS/IOU 61*
- *Rosemount Level Transmitters (14xx, 33xx, 53xx, 54xx, 56xx)*
- *Rosemount Radar Level Gauges (Pro, 39xx, 59xx)*
- *Rosemount Tank Radar Gauges (TGUxx)*
- *Rosemount Level Detectors (21xx)*
- *Emerson Aperio software*

The potential risks related to the vulnerabilities discussed in this Cyber Security Notification are lowered if the Affected Product is isolated from the internet and operating on a well-protected network consistent with

industry practice. Each user should consider their particular system configuration and circumstances and determine the effect of this issue as it relates to their application and take appropriate actions.

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.

Executive Summary

This is a proactive notification to inform end users that Emerson is aware of the recently disclosed Log4j vulnerability and are assessing how it affects our products. This notification is to inform end users that the products listed above are **not affected** by the Log4j vulnerability. This is an evolving situation, and this notification will be updated if new information becomes known.




Recommendations

Emerson continues to recommend following security best practices including protecting and segregating networks, keeping software and firmware up-to-date and other hardening guidelines.

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 Emerson Automation Solutions sales representative with any questions regarding this issue or for technical support. For additional assistance, use the following website:

- <https://www.emerson.com/en-us/contact-us>