

EMERSON CYBER SECURITY NOTIFICATION

ID number and revision	EMR.MSOL22001, revision 1	
Status and date	28-January-2022	
Affected Products:		
<ul style="list-style-type: none">Emerson Security Setup Utility, Version 1.6.8 and earlier. Fixed in version 1.6.9 and later.PlantWeb Insight, Version 2.3.4 and earlier. Fixed in version 2.3.5 and later.Emerson Version 4 WirelessHART Gateways, (1410, 1420, 1552, 1410D) Firmware version 4.8.0 and earlier. Fixed in version 4.8.1 and later.Emerson v6 WirelessHART Gateways (1410S) Firmware version 6.6.0 and earlier. Fixed in version 6.6.1 and later.		
Description	CVSS v3 Base Score	Vector
Gateway admin credential disclosure	8.8	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
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

A vulnerability has been discovered by researchers from the security firm, Dragos, that affects Emerson's Security Setup Utility, PlantWeb Insight, and Emerson Wireless Gateway products (both v4 and v6 models). The issue is related to a man-in-the-middle attack that could allow disclosure of gateway credentials. It is important to note that credential-disclosure can only occur when a secure connection is initiated and there is no further risk of disclosure after the secure connection is established. **Users can mitigate this issue by initiating the secure connection on a secure network prior to deploying to the field, by changing their password after the secure connection has been established or by upgrading the firmware and software for the affected products.**

It is important to remember that if the affected products are isolated from the internet and running on a well-protected network consistent with industry best practice, the potential risk is significantly lowered. Each user should consider their particular system configuration and circumstances and determine the effect of this potential issue as it relates to their application and take appropriate actions.

Risk Assessment

As mentioned above, this vulnerability was discovered by researchers from the security firm Dragos. The details of this vulnerability involve disclosure of the gateway credentials during the provisioning process. When a secure connection is established between the gateway and Security Setup Utility for the first time, or between the gateway and PlantWeb Insight for the first time, the gateway credentials are exchanged to ensure the connection is authorized. These credentials are not protected and sent in clear



text. Again, this only happens when the secure connection is established for the first time. Users can mitigate this issue by initiating the secure connection on a secure network prior to deploying to the field, by changing their password after the secure connection has been established or by upgrading the firmware and software for the affected products. Further details about the upgrade procedure can be found in the software release notes.

Emerson would like to thank the Dragos Team for practicing responsible disclosure and for providing time to issue updated firmware and software to address this issue. Responsible disclosure is critically important to ensuring the security of end users' networks and Emerson has appreciated the opportunity to work with these researchers to resolve these issues.

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.

Recommendations

Emerson recommends that users upgrade their software and firmware and change the gateway admin password. It is important that users upgrade the firmware and/or software on all affected devices to fully mitigate this issue by following the instructions in the software release notes.

Alternatively, users can also mitigate this issue by performing the secure connection on a separate, well-protected network that is known to be secure, or by changing their password after the secure connection has been established. It is also recommended that end users have a strong physical security program to ensure only authorized personnel have physical access to the facilities.

In addition, Emerson recommends continuing to follow the guidance given in Emerson's Wireless Security whitepaper which is freely available and can be downloaded here:

<https://www.emerson.com/documents/automation/emerson-wireless-security-wirelessmart-wi-fi-security-en-41260.pdf>

Software and Firmware Updates




The easiest and most convenient way to be notified about upcoming gateway firmware and Security Setup Utility software releases and to obtain information about the existing releases is to navigate to https://go.emersonautomation.com/rmt-en-w-wireless-gateway-firmware?utm_source=rmt_us-elqw-gf_arop&utm_medium=mixe&utm_content=upgrade_dl&utm_campaign=20grmtw-gateway_firmware01. Follow the form instructions and submit your request to be included in upcoming notifications, software/firmware updates and latest news. First time users will be prompted to create a free Guardian account for accessing updates.

For PlantWeb Insight, users should contact their Emerson sales representative or email PlantwebInsightSoftwareRequests@Emerson.com directly with a copy of their Purchase Order in order to receive digital download links for the latest version of their software.

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 Automation Solutions Global Response Center (24/7 Support)

Phone: +1 314 679 8984

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

Phone: 1-800-654-7768

3. Email to Rosemount Quality Feedback

RMT-NA.SpecialistWireless@emerson.com