EMERSON CYBER SECURITY NOTIFICATION

ROSEMOUNT XSTREAM DISCOVERED VULNERABILITIES

ID number and revision	EMR.RMT20006, revision 2
Status and date	18-May-2021

Affected Products: *The following Rosemount X-STREAM Continuous Gas Analyzers are impacted:*

X-STREAM enhanced XEGP – all revisions
X-STREAM enhanced XEGK – all revisions
X-STREAM enhanced XEFD – all revisions
X-STREAM enhanced XEXF – all revisions

CVE	CVSS	Vector
CVE-2021-27457	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2021-27459	7.1	AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:N
CVE-2021-27461	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVE-2021-27463	5.3	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVE-2021-27465	5.3	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVE-2021-27467	5.4	AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Executive Summary

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.

This notification is intended to inform end users that Emerson is aware of a number of vulnerabilities that affect the products listed above. Emerson has updated software to address these issues and is recommending that users upgrade firmware to resolve these issues. These vulnerabilities are in addition to those vulnerabilities disclosed in EMR.RMT20003 and EMR.RMT20005.

Emerson does not recommend connecting the Affected Products directly to the Internet. It is important to note that **if the Affected Product is isolated from the internet as recommended, and running on a well-protected network consistent with industry best practices, the potential risk is 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

These vulnerabilities initially discovered by internal testing performed by Emerson, are being disclosed as part of Emerson's responsible disclosure commitment to informing customers of known vulnerabilities. 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.

Six CVEs have been assigned:

CVE-2021-27457– The user credentials are kept using a weak encryption algorithm which allows an attacker to more easily gain the credentials used to login. Once these credentials are obtained unauthorized access to the device can allow the attacker to reconfigure the device or obtain other sensitive information.

CVE-2021-27459 – The application allows for certain files to be uploaded. It is possible to upload a malicious file into the web server system. This malicious file could then allow unauthorized access to sensitive data such as login credentials

CVE-2021-27461– Access to unauthorized data stored in the web server can be obtained by use of direct typing of the URL address into the web server. If the web server contains sensitive data, this data can be accessed using this technique.

CVE-2021-27463– When a session cookie attribute is not set properly unauthorized users who can intercept the cookies may gain access to information contained in the cookie.

CVE-2021-27465– A malicious user could inject arbitrary HTML code into a web page. This would allow an attacker to modify the page and display incorrect or undesirable data.

CVE-2021-27467– UI redress attack allows an attacker to route click or keystroke to another page provided by the attacker in order to gain unauthorized access to sensitive user information such as passwords.

Details of these vulnerabilities can be found on in CISA's ICS Advisory: ICSA-21-138-01.

Recommendations

Emerson recommends end users update the firmware on the Affected Products as soon as possible. A new release of the software that fixes the issues identified in this Cyber Security Notification is available. For update information contact TechSupport.Hasselroth@emerson.com.

In addition, Emerson recommends end users continue to utilize current cyber security industry best practices and action should be taken to ensure the Affected Product is connected to a well-protected network. The Affected Product should not be connected to the Internet.

One of the cyber security best practices should include configuring web browsers to prohibit storage of user information such as login name and password is disabled.

For more information on Emerson Security go to:
https://www.emerson.com/en-us/support/security-notifications

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.
ℹ	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: +1 888 889 9170

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

   Phone: 1-800-654-7768

3. **Email to Rosemount Quality Feedback**

   SpecialistCombustionAnalytical.rmtna@Emerson.com