

EMERSON CYBER SECURITY NOTIFICATION

ROSEMOUNT GC70XA REPORTED VULNERABILITIES

ID number and revision	EMR.MSOL23001, revision 2	
Status and date	8-February-2024	
Affected Products:	The following Rosemount Gas Chromatographs are impacted: GC370XA – version 4.1.5 and all prior revisions GC700XA – version 4.1.5 and all prior revisions GC1500XA – version 4.1.5 and all prior revisions	
CVE	CVSS	Vector
CVE-2023-46687	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-49716	8.3	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
CVE-2023-51761	6.9	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:H
CVE-2023-43609	6.9	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:H

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.

Emerson has been informed of vulnerabilities recently disclosed by an external researcher and verified by internal testing. The four vulnerabilities allow for an unauthenticated user with network access to run arbitrary commands in root context, to bypass authentication and acquire admin capabilities, get access to sensitive information, and run arbitrary commands. Additional information regarding these vulnerabilities can be found in CISA's ICS Advisory: [ICSA-24-030-01](#).

This notification is intended to inform end users that Emerson is aware of the vulnerability and has updated software to address the issue. 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

The vulnerability was initially discovered by Vera Mens of Claroty Research and is being disclosed as part of Emerson's commitment to our responsible disclosure to inform customers of known potential risks. 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.

There is four CVE's associated with this notification:

- CVE-2023-46687 Preauth Command Injection via Command 0x23 (gunzip)
This vulnerability allows an unauthenticated user with network access to arbitrary commands in root context from a remote computer.
- CVE-2023-49716 User Login Bypass via Password Reset Mechanism
This vulnerability allows an unauthenticated user with network access to bypass authentication and acquire admin capabilities.

- CVE-2023-51761 Firmware Does not Enforce Authorization Correctly
This vulnerability allows an unauthenticated user with network access to get access to sensitive information and even cause Denial of Service.
- CVE-2023-43609 Command Injection via Reboot Functionality (0x49)
This vulnerability allows an authenticated user with network access to run arbitrary commands from a remote computer.

Recommendations

Emerson recommends end users update the firmware on the Affected Products. A new release of software that addresses the issues identified in this Cyber Security Notification impacting the Affected Product is available. For update information contact GC Technical support at GC.CSC@emerson.com




In addition, Emerson recommends end users continue to utilize current cybersecurity industry best practices and in the event such infrastructure is not implemented within an end user's network, action should be taken to ensure the Affected Product is connected to a well-protected network and not connected to the Internet. 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 the 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: +1 888 889 9170
2. **Rosemount North American Response Center (24/7 Support – includes Canada)**
Phone: 1-800-654-7768
3. **Email to Rosemount Quality Feedback**
GC.CSC@emerson.com