



Bulletin No.: SQNSEC-2026-005	DATE OF ISSUE: 2026-08-21
SUBJECT: eCosPro RTOS Memory Allocator Integer Overflow (CVE-2021-27417)	
Author: Sequans Communications	Confidentiality: Public ☒ Private ☐
Contact: SEQUANS Communications Sales/FAE for further details	

1. Affected Products

Product series	Product name	Ordering code	Firmware version	Remarks
GC02S1	All variants	All	LR9.0.5.1 LR9.0.6.1 LR9.0.7.1	Under analysis
GM02S	All variants	All	LR8.2.2.1 and earlier	Under analysis
SKY66431	All variants	All	LR8.2.2.1 and earlier	Under analysis

1. Type

- ☐ Module / Hardware
- ☒ Firmware
- ☐ SDK / API
- ☐ Cloud / Service
- ☐ Tool / Application
- ☐ Other

2. Issue description

eCosPro RTOS (version 3.1.83), the real-time operating system underlying Calliope2/Monarch2 firmware, is potentially affected by an integer-overflow vulnerability in its memory-allocation routines (part of the industry-wide “BadAlloc” family of RTOS memory-allocator flaws disclosed in 2021).

CVE references:

- CVE-2021-27417

Impact statement:

The issue may allow memory corruption, denial of service, or potentially remote code execution, under the following conditions: a network- or RF-reachable code path must pass attacker-influenced size/count values into the affected allocation routine; a source-level audit of allocator call sites is in progress to confirm whether such a path exists in the shipped firmware.

At this stage, Sequans Communications has not identified evidence of exploitation in real-world deployments.



3. Recommendations

Sequans recommends customers to:

- This CVE is currently under internal analysis; a source-level audit of the firmware's allocator call sites is in progress.
- Sequans is engaging the eCosPro vendor to confirm patch/backport availability.
- Contact their Sequans representative for the latest status.

Available fix:

- Product: Calliope2 / Monarch2
- Firmware version: TBD — pending eCosPro vendor patch confirmation
- Availability date: TBD
- Delivery channel: Customer portal / direct support

Workaround:

- No workaround has been identified at this stage.

4. General security recommendations

Customers are advised to:

- Use secure communication protocols such as TLS where applicable.
- Keep device firmware up to date.
- Review product exposure and disable unused interfaces/services.
- Follow Sequans security guidance and customer release notes.

5. Reference documents

[1] NVD CVE-2021-27417 (nvd.nist.gov/vuln/detail/CVE-2021-27417)

[2] Sequans Customer Release Note (to be issued with fix)

[3] CISA / Microsoft “BadAlloc” advisory (2021)

For any question, please contact your Sequans sales or support representative.

6. Legal Notice

Copyright©2026, SEQUANS Communications

All information contained herein and disclosed by this document is confidential and the proprietary property of SEQUANS Communications and all rights therein are expressly reserved. Acceptance of this material signifies agreement by the recipient that the information contained in this document is confidential and that it will be used solely for the purposes set forth herein. Acceptance of this material signifies agreement by the recipient that it will not be used, reproduced in whole or in part, disclosed, distributed, or conveyed to others in any manner or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the express written permission of SEQUANS Communications.

 SEQUANS SECURITY/INFORMATION BULLETIN

All Sequans' logos and trademarks are the property of SEQUANS Communications. Unauthorized usage is strictly prohibited without the express written permission of SEQUANS Communications.

All other company and product names may be trademarks or registered trademarks of their respective owners. Products and services of SEQUANS Communications, and those of its licensees may be protected by one or more pending or issued U.S. or foreign patents.

Because of continuing developments and improvements in design, manufacturing, and deployment, material in this document is subject to change without notification and does not represent any commitment or obligation on the part of SEQUANS Communications. SEQUANS Communications shall have no liability for any error or damages resulting from the use of this document