



Bulletin No.: SQNSEC-2026-007	DATE OF ISSUE: 2026-08-21
SUBJECT: libcurl ASN.1 Certificate Parsing Out-of-Bounds Read (CVE-2024-7264)	
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

curl's generic X.509 ASN.1 parser (used by TLS backends that lack native certificate-field extraction) contains an out-of-bounds read when parsing a certificate's GeneralizedTime field. This applies only to specific TLS backends (GnuTLS, Schannel, SecureTransport, or mbedTLS from curl 8.9.0 onward); the exact TLS backend compiled into Calliope2/Monarch2's curl build is still being confirmed internally.

CVE references:

- CVE-2024-7264

Impact statement:

The issue may allow denial of service (process crash) while parsing a malicious TLS certificate, under the following conditions: curl must be built against an affected TLS backend for the parser to be reached; applicability to the shipped firmware build is under confirmation.

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 to confirm the compiled-in TLS backend for the shipped curl build.
- If confirmed applicable, Sequans will upgrade curl accordingly.
- Contact their Sequans representative for the latest status.

Available fix:

- Product: Calliope2 / Monarch2
- Firmware version: TBD — pending confirmation of the compiled-in TLS backend
- Availability date: TBD
- Delivery channel: Customer portal / direct support

Workaround:

- No workaround is currently available.

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-2024-7264 (nvd.nist.gov/vuln/detail/CVE-2024-7264)

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

[3] curl Security Advisory (curl.se/docs/CVE-2024-7264.html)

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