SECURITY/INFORMATION BULLETIN

Bulletin No.: SQNSEC-2026-006	**DATE OF ISSUE:** 2026-08-21
SUBJECT: libcurl Public Suffix List Domain-Matching Cookie Bypass (CVE-2023-46218)	
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 cookie engine, when built with Public Suffix List (libpsl) support, is susceptible to a mixed-case domain-matching bypass that could allow a malicious server to set an overly broad (“super”) cookie applicable to other domains. The firmware's cookie engine is confirmed active; whether the shipped build actually links libpsl is still being confirmed.

CVE references:

- CVE-2023-46218

Impact statement:

The issue may allow cross-domain cookie injection, under the following conditions: the shipped curl build must be linked against libpsl for this issue to be exploitable; this is currently under internal verification. 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 whether libpsl is linked in the production build.
- If confirmed linked, Sequans will upgrade curl to version 8.5.0 or later.
- Contact their Sequans representative for the latest status.

Available fix:

- Product: Calliope2 / Monarch2
- Firmware version: TBD — pending confirmation of libpsl linkage; if applicable, curl >= 8.5.0
- 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-2023-46218 (nvd.nist.gov/vuln/detail/CVE-2023-46218)

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

[3] curl Security Advisory (curl.se/docs/CVE-2023-46218.html)

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

6. Legal Notice