CRA Reporting Form

NEWLIFT
NEUE ELEKTRONISCHE WEGE

Cybersecurity Incident / Vulnerability in Lift Controllers

Please send report to: security@newlift.de
If urgency is "Critical" (section 8), also call immediately: 089 898660

Brief instructions for completion:

- Enter only known facts. Clearly mark assumptions as assumptions.
- State the time and the installation as precisely as possible.
- For a vulnerability, describe what was found and under which conditions.
- If you suspect an attack or manipulation, you do not have to "prove" anything – the suspicion and the observation are sufficient for a report.
- Do not make any changes of your own to software, firmware or safety-relevant parameters unless this is required by the applicable service instructions.
- If possible, secure photos, screenshots, error messages and logs without changing or deleting existing data.
- If information is uncertain, enter "unknown" or "unclear" – do not fill in fields with guesses.
- If a safety function may be impaired, escalate the situation to the VRT (Vulnerability Response Team) by phone immediately – do not wait to complete this form first.
- Whether a CRA reporting obligation exists is assessed exclusively by the VRT.

1 Reporting Person

Name	_____
Company / Department	_____
Role	☐ Customer / Operator ☐ Service technician ☐ NEWLIFT employee ☐ External security researcher ☐ Other: _____
Phone	_____
Email	_____
Date / time of discovery	_____
Date / time forwarded to NEWLIFT	_____
Do you wish to be named as the reporter in a later security advisory?	☐ Yes ☐ No (anonymous)

2 Affected Installation

Customer / Operator	_____
Installation number	_____
Location (address)	_____
Country	_____
Controller type	_____
Controller serial number (if known)	_____
Hardware version (if known)	_____
Software version (if known)	_____
Safety module (if known)	_____
Remote maintenance available	☐ Yes ☐ No ☐ Unknown
Network connection	☐ Internet / LAN ☐ Mobile network ☐ Emergency call system ☐ None ☐ Unknown
Other installations with the same controller / software version known?	☐ Yes, number: _____ ☐ No ☐ Unknown

3 What Was Observed?

- ☐ Suspected cyberattack
- ☐ Manipulation of parameters
- ☐ Malware / virus
- ☐ Unusual network communication
- ☐ Loss / theft of a service device
- ☐ Unauthorised access
- ☐ Manipulation of software / firmware
- ☐ Vulnerability discovered
- ☐ Loss of credentials
- ☐ Other

Description of the observation:

What happened? What was observed? When and under what circumstances?

Is there any indication that the vulnerability is already being exploited or is known to third parties?

e.g. observed attack, publication on the internet, notice from a third party

☐ Yes ☐ No ☐ Unknown

If yes, which indications:

4 Impact

- ☐ No known impact
- ☐ Safety function possibly impaired
- ☐ Remote maintenance impaired
- ☐ Parameters changed
- ☐ Installation out of service
- ☐ Persons at risk / trapped
- ☐ Data loss
- ☐ Other impact

Description of the impact:

What no longer works, or what could be affected?

5 Measures Already Taken

- ☐ Installation secured / taken out of service
- ☐ Customer informed
- ☐ Screenshots taken
- ☐ Data backup performed
- ☐ Other
- ☐ Remote access disabled
- ☐ Logs secured
- ☐ Photos taken
- ☐ No measures taken

Explanation:

Important: *Do not make any independent changes to safety-relevant parameters, software or firmware unless expressly instructed to do so.*

6 Available Evidence

- ☐ Photos
- ☐ Log files
- ☐ Service report
- ☐ Other documents
- ☑ Screenshots
- ☑ Error messages
- ☑ Network / system information

File names / storage location:

7 Initial Assessment – Is a Cybersecurity Connection Possible?

☐ Yes ☐ No ☐ Unclear

Reasoning / observation:

Why is there a suspicion?

8 Urgency / Possible Safety Impact

- ☐ **Critical:** safety function possibly impaired / immediate risk → **report by phone immediately**
- ☐ **High:** possible unauthorised access or manipulation
- ☐ **Medium:** suspicion or vulnerability without apparent immediate safety impact
- ☐ **Low:** other anomalies
- ☐ **Unclear**

If in doubt, report rather than not report.

Note

You do not need to determine whether a cyberattack has actually occurred. If you notice an unusual digital anomaly, an unexpected change, suspicious access or a possible vulnerability, please report it. Describe as precisely as possible what you observed. The technical and legal assessment will then be carried out by the VRT.

Data Protection

Your information will be processed exclusively for handling this report and for fulfilling legal obligations, in particular under Regulation (EU) 2024/2847 (Cyber Resilience Act), and will only be passed on to competent authorities to the extent necessary. Further information: https://www.newlift.de/datenschutz.html

If recorded by phone:

Recorded by _____ Date / time _____