

CA-000001

Cybersecurity Advisory: Security Update for LID-3300IP and LID-3300IP Type 2 Devices

Dear Customer,

Please ensure that your ice detection device is running at least firmware version V2.20 (released October 2021) and that HTTPS is activated. Older devices do not meet all current security requirements allowing targeted attack to the devices visible on the public Internet.

For more information and update instructions, please contact Labkotec sales (sales@labkotec.fi) or service (service@labkotec.fi).

This does not compromise personal data or financial information.

This concerns devices without HTTPS protection.

This does not apply to devices whose Ethernet connection is not connected.

Background

Vulnerability in ice detector software enables an unauthenticated attacker to alter device parameters and run operational commands, by sending a specially crafted packets to the device.

Devices that are not connected to an Ethernet network are not vulnerable to this attack.

Ice detectors connected to a secure internal network that follows modern security recommendations, where only authorized devices and users can communicate with the ice detector, are protected from external attacks.

1. Update Requirement

Labkotec recommends updating ice detectors to the LID-3300IP Type 2 model and installing the latest firmware version V2.40. It is also highly recommended to activate HTTPS for network traffic.

2. Device Types and Limitations

- LID-3300IP: It is not possible to implement secure and encrypted network traffic.
- LID-3300IP Type 2: Firmware V2.20 and newer support secure and encrypted network traffic.
 - Requires HTTPS activation.

You can check the device type and software version in the web interface.

3. Additional Instructions and Security

- The device must not be connected to the public internet.
- Follow good security practices
- Change Default Credentials
 - Replace all factory-set usernames and passwords with strong, unique credentials immediately after installation.
- Enable Secure Management Access
 - Activate HTTPS encryption for the device's management interface to protect data in transit.
- Network Segmentation
 - Place IoT devices on dedicated network segments designed specifically for automation systems. Avoid mixing with general-purpose networks.
- Implement Firewall and Access Controls
 - Configure firewalls to restrict access to these segments. Only allow approved endpoints or authenticated users to connect to devices.
- Restrict Protocols
 - Permit only necessary communication protocols. Detailed information of the used protocols can be found from the manuals.
- Monitor and Alert
 - Log all network traffic to and from the device. Where possible, set alerts for unusual activity or if the device unexpectedly disconnects from the network.
- Avoid Direct Internet Exposure
 - Do not connect devices directly to the public internet. If remote access is required, use a well-maintained VPN solution as a secure gateway.
- Keep Firmware Updated
 - Regularly apply firmware and security updates—at least annually or as recommended by the manufacturer.
- Control Physical Access
 - Restrict physical access to device installation sites to authorized personnel only.
- Maintain Inventory and Access Reviews
 - Keep a complete inventory of all devices. Track configuration changes and periodically review user access lists and credential management.

4. Impact of a Security Incident

- Does not compromise personal or financial data.
- Attacker can change the ice detector behaviour by altering the configuration remotely.
- The vulnerability concerns devices without HTTPS protection.
- Devices not connected via Ethernet are not affected by the issue.

Best regards,
Labkotec Oy