Coordinated Vulnerability Disclosure Process

Telemecanique Sensors welcomes reports of potential security vulnerabilities affecting its products with digital elements.

How to report

Potential vulnerabilities may be reported to: **cybersecurity@tesensors.com**
Additional product cybersecurity information is available at: **https://www.telemecaniquesensors.com/global/en/support/product-cybersecurity**

What to include

To help us investigate, please provide, where available:

- affected product name, reference, and version
- description of the issue and potential impact
- steps to reproduce
- logs, screenshots, or proof-of-concept details where relevant
- your contact details and preferred method of communication

Our approach

We review reported vulnerabilities and may contact the reporter for additional information. **We aim to acknowledge receipt of vulnerability reports within 7 calendar days** and to maintain communication during the assessment and handling process as appropriate.

Where appropriate, **Telemecanique Sensors** may assign a tracking identifier to facilitate follow-up communication.

Coordinated disclosure

We ask reporters to **avoid public disclosure of vulnerability details before we have had a reasonable opportunity to assess the report** and, where appropriate, prepare mitigation guidance or a remediation. Disclosure timing may be coordinated depending on the nature of the issue and the parties involved.

Communication to customers and users

Where relevant**, Telemecanique Sensors** may communicate vulnerability-related information, mitigations, and security updates through product pages, website notices, advisories, direct email, or other appropriate channels.

YAGEO Business Confidential: This document is Business Confidential and should not be reproduced, copied or given to a third party without the express written permission of YAGEO Corporation