PRODUCT SECURITY

Cyber Resilience Act (CRA) & Product Security

Regulation (EU) 2024/2847

COMMITMENT TO CYBERSECURITY

MACSA ID is committed to developing and maintaining secure products and services in accordance with recognized cybersecurity best practices and the requirements of the EU Cyber Resilience Act (Regulation (EU) 2024/2847). The security of our customers, partners, and users is a core element of our product lifecycle.

SECURITY BY DESIGN

Security is integrated throughout the design, development, testing, deployment, and maintenance phases of our products.

Our security practices include:

- Secure development processes
- Risk-based security assessments
- Vulnerability management and remediation
- Security testing and validation
- Controlled release of security updates
- Continuous monitoring of relevant security threats

These measures help us identify, assess, and reduce cybersecurity risks throughout the product lifecycle.

VULNERABILITY DISCLOSURE

We welcome reports from security researchers, customers, and partners who identify potential security vulnerabilities in our products or services.

To report a vulnerability, please contact:

PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT)

psirt@macsa.com

The information submitted must be in Spanish or English.

To ensure we can evaluate and process the notification as quickly as possible, please include the following information in the notification:

1. Product name, model and serial number.
2. Software or firmware version and configuration.
3. A clear and detailed description of the identified vulnerability or issue.
4. Steps to reproduce it.
5. Evidence to facilitate validation (e.g., configuration details, screenshots, logs, or information on how to exploit the vulnerability).
6. An assessment of the potential impact.
7. Contact details for follow-up on the case.

MACSA ID respects the confidentiality of those who submit notifications and will not disclose their personal data without their explicit consent, unless necessary for managing the vulnerability.

COORDINATED VULNERABILITY DISCLOSURE POLICY

We support responsible and coordinated vulnerability disclosure.

Upon receipt of a vulnerability report, we aim to:

1. Acknowledge receipt of the report.
2. Assess and validate the reported issue.
3. Determine appropriate remediation measures.
4. Coordinate communication with the reporting party where appropriate.
5. Inform affected users and publish security information when relevant.

We request that researchers:

- Act in good faith.
- Avoid accessing, modifying, or deleting data.
- Avoid disrupting services or systems.
- Allow reasonable time for remediation before public disclosure.

The objective of this process is to protect users while ensuring vulnerabilities are remediated in a responsible manner.

SECURITY INFORMATION

Current security information may include:

- Security advisories
- Vulnerability notifications
- Product security notices
- Update and patch information
- Product security contact details