MACHINERY
SERVICES
PACKAGING
COATING
INSPECTION

AISA

Vulnerability Report Form

Use this form to report a suspected security vulnerability affecting an Aisa product, software, firmware, service, or related component. Fields marked with * are required.

Note: Provide enough detail for Aisa to understand, reproduce, and assess the issue. Where possible, attach proof-of-concept material, screenshots, logs, packet captures, or other supporting evidence. Avoid including unrelated personal or confidential data.

1 REPORTER DETAILS

Name or researcher alias / Organisation	Email / contact address *

Public credit / attribution preference

☐ Yes, I would like public credit ☐ No public credit

Name / alias to use for attribution *Complete if public credit is requested*

2 VULNERABILITY SUMMARY

Vulnerability title * *Short, descriptive title*

Brief vulnerability description * *Summarize the issue and why it matters*

Vulnerability category *

- ☐ Authentication
- ☐ Injection / Corruption
- ☐ Information Disclosure / Data Exposure
- ☐ Denial of Service / Availability
- ☐ Memory Safety / Corruption
- ☐ Debug / Maintenance / Engineering Interface
- ☐ Third-party Component / Dependency
- ☐ Authorization / Access Control
- ☐ Cryptography / Key & Certificate Management
- ☐ (Remote) Code / Command Execution
- ☐ Configuration / Insecure Default
- ☐ Firmware / Software Update & Integrity
- ☐ Physical / Local Interface Security
- ☐ Other / Unknown:

Date of discovery	Reference / ticket held by reporter

Initial attack scenario / security concern *In one or two sentences, describe how the vulnerability could be triggered or abused*

Other summary information

3 AFFECTED ASSET / PRODUCT

Affected machine / product / system * *Product family, machine model, software, firmware, service, etc.*

Equipment serial number *

Component software version *

URL / endpoint / network interface *if known*

Protocol / service / port *if known*

Environment / configuration *Relevant operating conditions, deployment mode, connected systems, access path, or configuration*

Other potentially affected products or versions *Include any scope uncertainty*

AISA Automation Industrielle SA
Avenue de Savoie 61 – P.O. Box 336 – CH-1896 Vouvry (VS) – Switzerland ■ Tel. +41 24 4820 110 ■ www.aisa.com

4 TECHNICAL DETAILS

Detailed technical description * *Explain the vulnerability, root condition if known, and affected attack surface*

Preconditions / prerequisites * *Required access, configuration, credentials, network position, privileges, physical access, etc.*

Steps to reproduce * *Numbered steps are preferred; include exact requests, commands, inputs, or sequences where relevant*

Expected result * *Normal or secure behaviour*

Actual result * *Observed vulnerable behaviour*

Proof of concept / technical evidence * *Paste concise PoC details or reference attached code, captures, logs, screenshots, etc.*

Workarounds / mitigation suggested by the reporter *Optional*

5 IMPACT & EXPLOITATION

Potential security impact * *Describe what an attacker could achieve and the affected security properties*

Authentication required?

- ☐ Yes
- ☐ No
- ☐ Unknown

Privileges required?

- ☐ None
- ☐ Low / standard user
- ☐ High / administrator
- ☐ Unknown

User interaction required?

- ☐ Yes
- ☐ No
- ☐ Unknown

Has exploitation been observed? *

- ☐ Yes
- ☐ No
- ☐ Unknown

If yes, describe the observed exploitation *When, where, and how it was observed; include evidence if available*

Reporter-assessed severity *Aisa will determine a final severity level*

- ☐ Critical
- ☐ High
- ☐ Medium
- ☐ Low
- ☐ Unknown / not assessed

Potential impact areas

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Safety

6 DISCLOSURE & COMMUNICATION

Reported to another organisation?

☐ Yes ☐ No

If yes, identify the organisation(s) and reference(s) *Where disclosure would create confidentiality concerns*

Are other vendors / products potentially affected?

☐ Yes ☐ No
☐ Unknown

Known CVE identifier *If already assigned*	**Planned publication date** *If applicable*

Do you intend to publish details?

☐ Yes ☐ No
☐ Undecided

Additional information *Anything else that would help coordinate validation, remediation, or disclosure*

SUBMISSION CHECK

☐ I have provided sufficient information to reproduce or assess the issue where reasonably possible.
☐ I have identified or referenced supporting evidence and attachments.
☐ I have stated any known or planned disclosure to third parties or the public.

Submit this form to otcybersecurity@aisa.com.
Do not send exploit code or sensitive evidence through an unsecured channel if a secure reporting option is available.

Date of submission