Coordinated Vulnerability Disclosure Policy

1. Purpose

Gasparini S.p.A. considers the responsible disclosure of vulnerabilities to be an essential part of the cybersecurity process for its products.

This policy describes how customers, security researchers, partners, suppliers and other parties can report a potential vulnerability to Gasparini S.p.A., what information is useful to enable its analysis, and how the subsequent coordination is handled.

The aim is to enable Gasparini S.p.A. to verify the issue, identify the affected products and versions, and prepare any corrective or mitigating measures before detailed technical information is made public.

This policy is the public point of reference for reporting vulnerabilities affecting Gasparini S.p.A. products.

2. Scope

This procedure may be used to report cybersecurity vulnerabilities or weaknesses affecting Gasparini S.p.A. products that contain digital components, including, where applicable:

- application software;
- HMI software;
- firmware;
- operating systems and their configurations, when supplied as part of the machine;
- services and software components developed by Gasparini S.p.A.;
- third-party libraries and software components integrated into the product;
- network interfaces, protocols and services exposed by the product;
- authentication and authorisation mechanisms;
- remote update or maintenance functions;
- configurations that may affect the security of the product.

A vulnerability in a third-party component may be reported to Gasparini S.p.A. when that component is used within a Gasparini S.p.A. product. In such cases, Gasparini S.p.A. will assess the impact on its own products and, where necessary, coordinate the handling of the issue with the manufacturer or maintainer of the component.

Requests for technical assistance that do not concern a cybersecurity issue should instead be directed to the standard Gasparini S.p.A. support channels.

3. How to report a vulnerability

Vulnerabilities can be reported through the following point of contact:

Web page: https://www.gasparini-spa.com/de/service/cybersicherheit/

This point of contact should be used exclusively or primarily for matters relating to product cybersecurity, so that reports can be promptly handled by the designated staff.

For particularly sensitive technical information, a secure communication channel will be available:

PGP-encrypted e-mail

The web page dedicated to reporting shall make available both this policy and the information needed to use the secure channel.

4. Information to include in the report

A report should nevertheless contain sufficient information to enable Gasparini S.p.A. to understand the issue and begin its analysis.

Where available, it is helpful to provide:

- serial number
- description of the vulnerability
- component in which the issue was identified
- conditions required to reproduce the vulnerability
- steps taken to verify the vulnerability
- possible impact on the safety of the machine and/or the operator
- any proof-of-concept code, logs, screenshots or other technical evidence (as file attachments)
- information on whether the vulnerability is publicly known or being exploited
- Contact information (e-mail address)

The reporter should also provide contact details that allow Gasparini S.p.A. to request clarification during the analysis.

It is not necessary to submit personal data, credentials, confidential customer information or any other data that is not strictly necessary to demonstrate the vulnerability.

5. Handling of reports

Gasparini S.p.A. records the reports it receives and carries out an initial assessment to determine whether the issue described concerns a product within its scope and whether the information available is sufficient to proceed with the analysis.

Where the reporter has provided valid contact details, Gasparini S.p.A. acknowledges receipt of the report and may request further information or technical evidence.

The subsequent analysis may include reproducing the issue, identifying the affected versions and components, assessing the impact and defining possible corrective measures.

Where the vulnerability concerns a component developed or maintained by a third party, Gasparini S.p.A. may involve the relevant manufacturer, supplier or maintainer, limiting the information shared to what is necessary to analyse and resolve the issue.

The time required for analysis and remediation depends on the nature of the vulnerability, its complexity, the products affected and the availability of a mitigation or update.

Gasparini S.p.A. will, as far as possible, keep in contact with the reporter throughout the main stages of handling the case.

6. Coordinated disclosure

Gasparini S.p.A. asks those who report a vulnerability not to publish technical details that could facilitate its exploitation before the issue has been analysed and a corrective or mitigating measure has been made available.

Where public disclosure is planned, Gasparini S.p.A. and the reporter may agree on the timing and manner of publication, taking into account:

- the severity of the vulnerability;
- the likelihood and ease of exploitation;
- any evidence of active exploitation;
- the availability of workarounds;
- the availability of a security update;
- the time reasonably required for users to apply the fix;
- any involvement of other manufacturers or vulnerable components.

The request for coordination is not intended to prevent the disclosure of a vulnerability, but to reduce the risk to users during the time needed to analyse and fix it.

When a security update is released, Gasparini S.p.A. may make information available to enable users to identify the affected product, understand the impact of the vulnerability and take the necessary measures.

7. Expected conduct during research activities

Gasparini S.p.A. asks anyone conducting security research on its products to act in a manner proportionate to the need to verify the existence of the vulnerability.

In particular, verification should not involve:

- intentional access to personal data or confidential information not required for the research;
- modification or deletion of data;
- permanent alteration of the product configuration;
- deliberate disruption of services or production processes;
- compromise of systems belonging to customers or third parties;
- installation of persistence mechanisms;
- use of the vulnerability to gain further access beyond what is necessary to demonstrate its existence;
- activities that could endanger the physical safety of people, machinery or plants.

If personal data, credentials or other confidential information are accidentally discovered during verification, the activity should be stopped once the minimum evidence needed to demonstrate the issue has been collected. Such information should not be retained, used or disclosed beyond what is strictly necessary for the report.

Particular care must be taken with industrial machines in operation. Security testing must not introduce risks to people, plants, production or the environment.

8. Known vulnerabilities and third-party components

The presence of a publicly known vulnerability in a component used by a Gasparini S.p.A. product does not automatically mean that the product is vulnerable.

Where possible, the report should explain why the vulnerability is considered applicable to the Gasparini S.p.A. product, specifying the component and version affected.

Gasparini S.p.A. will assess the actual exposure of the product and the conditions required for exploitation.

Where a vulnerability originates from a third-party component, handling may require coordination with the relevant supplier before a fix can be made available.

9. Communications and acknowledgement of the reporter

Where appropriate and with prior consent, Gasparini S.p.A. may publicly acknowledge the contribution of the researcher or party who reported the vulnerability.

The decision to credit the reporter is agreed before the publication of any security advisory or other public communication.

This policy does not constitute a bug bounty programme and does not automatically provide for rewards or financial compensation for reported vulnerabilities.

10. Incomplete, irrelevant or unverifiable reports

Gasparini S.p.A. may close a report when:

- the issue does not concern a Gasparini S.p.A. product;
- it is not possible to obtain sufficient information to understand or reproduce it;
- the reported behaviour does not constitute a cybersecurity vulnerability;
- the issue is already known and is already being handled;
- the report relates solely to a request for technical assistance.

Where possible, the reason for closure is communicated to the reporter.

A closed report may be reassessed if new technical evidence is subsequently provided.

11. High-impact or actively exploited vulnerabilities

A report indicating possible active exploitation, a compromise that has already occurred or a significant impact on product safety is treated as a priority.

Gasparini S.p.A. may promptly request further information from the reporter and activate its internal escalation and vulnerability management procedures and, where applicable, fulfil the obligations laid down by applicable legislation.

The reporting process set out in this policy is separate from any regulatory obligations to notify the competent authorities, which are handled internally by Gasparini S.p.A.

12. Protection of information received

Information concerning vulnerabilities that have not yet been fixed must be handled with particular care.

Gasparini S.p.A. restricts access to technical details to those who need such information to analyse the issue, develop a fix, coordinate with any parties involved or comply with regulatory obligations.

Where handling the vulnerability requires the involvement of suppliers, partners or other manufacturers, only the information necessary to manage the issue is shared.

13. Policy updates

This policy is reviewed whenever there are changes to the reporting channels, the internal vulnerability handling process or the applicable regulatory requirements.

The current version must be available on the Gasparini S.p.A. website together with the point of contact used for reports.

References

This policy has been drawn up taking into account the vulnerability handling requirements of **Regulation (EU) 2024/2847, Cyber Resilience Act**. Annex I, Part II requires manufacturers to put in place and enforce a coordinated vulnerability disclosure policy and to facilitate the sharing of information about vulnerabilities, including by providing a contact address for reporting them. Annex II further requires that the information supplied with the product indicate the single point of contact where vulnerabilities can be reported and the related policy can be found.

The following was also considered as a technical reference: **prEN 40000-1-3:2025, Vulnerability Handling Requirements**, in particular with regard to the CVD policy, secure communication and the capability to receive and handle reports. At the time of writing, the document is still a draft standard and has not been cited in the Official Journal of the European Union; it therefore does not yet confer a presumption of conformity with the CRA.

Status: Approved [sb]
Version: 0.3 [sb]
Organisation: Gasparini S.p.A.
Classification: Public