1 Coordinated Vulnerability Disclosure

Thomas GmbH, hereinafter referred to as Thomas, takes vulnerability reports seriously. If you find a potential vulnerability in Thomas products, IT systems, websites or services, please report it responsibly. Thomas will review your report, coordinate remediation and provide information about necessary measures.

The purpose of this policy is to handle vulnerabilities responsibly, confidentially and in a coordinated manner, reduce risks for users, customers, products and systems, and enable appropriate remedial measures.

The coordinated disclosure process may involve reporting persons, Thomas as the manufacturer or operator, affected third parties and responsible coordination bodies.

2 What can be reported?

You can report potential vulnerabilities in products, IT systems, websites or services that are manufactured, provided or operated by Thomas. This includes vulnerabilities that may affect confidentiality, integrity or availability.

Vulnerabilities in products, components, systems or services of third-party providers, service providers or suppliers are generally not within the direct scope of this policy. Such vulnerabilities must be reported directly to the respective provider or the responsible coordination body. Do not perform active tests if it is unclear whether a product or system falls within the scope; in this case, contact Thomas first.

General support requests, feature requests, questions about product availability and non-security-related defects are not handled through this procedure. Please use the contact options on our website for these matters.

3 How to report a vulnerability

Please use the following reporting forms for your report:

- for vulnerabilities in products https://www.thomas-group.com/en/contact/#vulnerability
- for vulnerabilities in IT systems, websites or services https://www.thomas-group.com/en/contact/#security

Alternatively, send vulnerabilities in products to psirt@thomas-group.com and vulnerabilities in IT systems, websites or services to csirt@thomas-group.com.

Reports may be submitted anonymously. Please note that anonymous reports can only be processed to a limited extent, or possibly not at all, if follow-up questions, evidence or technical clarifications are required.

4 What your report should contain

Please describe the vulnerability as clearly and comprehensibly as possible. The following information is helpful:

- affected system, product, component, control unit or software module, preferably including name, HW/SW version and serial number
- a brief description of the vulnerability and steps to reproduce it
- possible impacts (confidentiality, integrity, availability, safety and/or privacy protection impact)
- date of discovery and available evidence such as proof of concept, reports, logs, screenshots or network captures
- whether the vulnerability is already publicly known or has been shared with third parties (e.g. reference to CVE identifiers)
- whether the vulnerability is already being actively exploited
- and your contact details for follow-up questions (unless the report is to be submitted anonymously).

Do not send personal data, passwords or confidential content.

Automated reports or scan results should only be submitted if they have a specific connection to a vulnerability and are explained in sufficient technical detail.

5 Please observe the following when testing

Act carefully and only to the extent necessary. Avoid disruptions, data changes, unauthorized access, privilege escalation, disclosure of confidential information and tests that could affect Thomas or third parties. Do not access third-party data and do not modify, copy, store or delete it. Exploits or verification methods may only be used to the extent necessary to confirm the vulnerability; in particular, not for data compromise or exfiltration, establishing persistent access, privilege escalation or accessing additional systems.

Prohibited testing methods include:

- social engineering, phishing or deception of employees, customers or third parties
- physical attacks, manipulation of buildings, facilities, devices or access controls
- denial-of-service, load or stress tests and measures that may affect availability, integrity or operations
- spam, brute-force attacks, credential stuffing or the use of malware
- accessing, modifying, copying, storing, deleting or disclosing third-party data

As soon as you have confirmed a vulnerability or encounter sensitive data, in particular personal data, financial information, confidential information or trade secrets, please stop your testing, inform Thomas immediately and do not disclose this data to third parties.

6 How Thomas handles your report

Thomas confirms receipt of your report within a reasonable time. Thomas then reviews the report, assesses the risk and impact, involves the responsible teams and plans appropriate measures. We will keep you informed accordingly, of course.

The coordinated vulnerability disclosure process generally ends when the report is unfounded, the vulnerability has been resolved or appropriately mitigated, or a remedial measure is available. If contact details are available, Thomas informs the reporting person about key steps.

7 Coordinated Vulnerability Disclosure

Do not publish technical details before Thomas has reviewed the vulnerability and implemented or agreed appropriate measures. Thomas coordinates the timing and scope of publication with you, affected third parties and responsible bodies, where possible.

8 Handling responsible reports

We will not take legal action against security researchers who:

- act in good faith
- follow this policy
- do not exfiltrate data or damage systems.

This requires that your activities serve solely to identify, verify and report security vulnerabilities and remain limited to what is necessary. This does not apply to actions that go beyond responsible security testing or violate applicable law. Thomas cannot make commitments on behalf of third parties, in particular customers, suppliers, service providers, authorities or other rights holders.

9 Privacy protection

Avoid accessing personal data. If you unintentionally see personal data, do not store, copy or publish it and inform Thomas immediately.

Thomas uses personal data from your report only for processing, communication and compliance with legal obligations. Further information on the processing of personal data can be found in Thomas's privacy policy (www.thomas-group.com/en/privacy-protection).