



Product Cyber Security and Responsible Disclosure Policy

Last updated: July 2026

Legal Compliance: Regulation (EU) 2024/2847 (Cyber Resilience Act)

Entity: MANITOWOC

1. Introduction and Regulatory Commitments

The security of our products is a top priority. In accordance with the European Cyber Resilience Act (CRA), MANITOWOC is committed to ensuring a high level of cybersecurity for all its products containing digital elements.

We acknowledge the crucial role that security researchers, partners, and customers play in proactively identifying threats. This policy outlines our responsible disclosure framework and specifies our legal obligations regarding transparency, vulnerability tracking, and the provision of security patches.

Our dedicated Product Security Incident Response Team (PSIRT) serves as the single point of contact to centralize reports, coordinate corrective actions, and liaise with European authorities (such as ENISA and national CERTs).

2. Scope

This policy covers all hardware and software products placed on the European market by MANITOWOC. This includes connected devices, embedded software, and associated applications.

Not in scope:

- Vulnerabilities affecting our internal IT infrastructures or MANITOWOC corporate websites.
- Standard technical support or customer service requests.
- Products that have officially reached their end-of-life and exceeded their guaranteed security support period.
- Vulnerability reports for issues that are already known, publicly disclosed, or previously reported by a third party.



3. Company Commitments (CRA Compliance)

To ensure the security of our users and comply with European legislation, we commit to the following:

- Providing free security updates: We will deploy security patches at no additional cost throughout the expected lifetime of the product (as defined at the time of purchase).
- Complying with legal reporting deadlines: In the event of an actively exploited vulnerability or severe incident, our PSIRT will notify ENISA and the competent national authorities within 24 hours (early warning), followed by a triage report within 72 hours.
- Maintaining transparency (SBOM): We maintain a Software Bill of Materials (SBOM) for each product to rapidly identify vulnerable third-party components.
- Non-retaliation: MANITOWOC will not take any legal action against security researchers who report vulnerabilities in good faith and in strict compliance with this policy.
- Protecting your anonymity: Reports can be submitted completely anonymously or under a pseudonym.

4. Responsible Disclosure Guidelines

If you identify a security flaw in any MANITOWOC product, we ask that you adhere to the following responsible disclosure guidelines:

- Report promptly: Inform us as soon as possible using our secure contact form.
- Provide detailed documentation: Include comprehensive technical evidence (screenshots, code snippets, reproduction steps) to facilitate analysis by our PSIRT.
- Responsible testing: Only test for security issues on devices, systems, or accounts that you own (or for which you have explicit permission from the owner).
- No disruption or alteration: Any attempt to gain unauthorized access, exfiltrate customer data, or disrupt our services (e.g., DDoS attacks) is strictly prohibited.
- Strict confidentiality: To allow us adequate time to develop a patch and meet our regulatory deadlines, do not disclose any information to the public or third parties without prior written consent from MANITOWOC.

5. Vulnerability Handling Process

1. Receipt: Upon submission of your report via our form, our team will acknowledge receipt within a maximum of five business days.
2. Analysis (Triage): The PSIRT will verify the validity of the vulnerability in coordination with our development teams. If further information is needed, we will contact you directly.
3. Legal Obligations (if applicable): If the vulnerability is deemed critical or is actively exploited, we will immediately trigger the regulatory reporting protocol via the ENISA Single Reporting Platform within the 24-to-72-hour timeframe.
4. Remediation: The PSIRT will coordinate the creation and deployment of a security update (patch) or an appropriate mitigation measure.
5. Closure and Disclosure: Once the product has been secured, MANITOWOC will inform you of the resolution. A final report will also be submitted to regulatory authorities within 14 days of deploying the fix, as mandated by the CRA.



DE DDY DG 0017-00

6. Contact Information

To submit a vulnerability report or to ask questions regarding this policy, please contact the PSIRT via our dedicated form. Communications may be submitted in English, French, or German.

Corporate Headquarters:
MANITOWOC Crane Group France
66 Chemin du Moulin Carron, 69570 Dardilly.
Website: <https://www.manitowoc.com/>
Contact: psirt@manitowoc.com

We sincerely appreciate the cybersecurity community's valuable collaboration in helping us continuously improve the security of our products.