Responsible Disclosure Policy

Our Responsible Disclosure Policy is committed to ensuring the safety and security of our assets, systems, and customers' information. If security researchers identify potential vulnerabilities in any of our products, systems, or assets, we encourage them to contact us immediately through our Responsible Disclosure Program. We appreciate your submission, but we do not offer rewards or compensation for identifying potential issues since we do not have a public bug bounty program.

Responsible Disclosure Program Guidelines

To disclose potential vulnerabilities responsibly, researchers must adhere to the following guidelines:

- → Do not engage in any activities that may cause harm to We Can, our customers, or employees.
- → Do not engage in any activities that may degrade our services or assets or cause them to stop functioning.
- → Do not violate any applicable laws or regulations or the laws or regulations of any country where data, assets, or systems reside, data traffic is routed, or where the researcher is conducting research activity.
- → Do not put We Can in violation of any applicable laws or regulations or the laws or regulations of any country where data, assets, or systems reside, data traffic is routed, or where the researcher is conducting research activity.
- → Do not store, share, compromise, or destroy any We Can or customer data. If any Personal Information is identified, immediately stop the activity, remove related data from your system, and contact us immediately.
- → Do not initiate fraudulent financial transactions.
- → Do not disclose any reported issues to third parties or publish them publicly.

We commit to providing prompt acknowledgement of receipt of all reports within five business days of submission. We shall use commercially reasonable endeavors to keep you reasonably informed of the status of any validated vulnerability that you report through this program.

Submission Format

To report a potential vulnerability, please include a detailed summary of the vulnerability, including the target, steps, tools, and artifacts. Screen captures may also be included to illustrate details.

Physical testing of premises

Please note that certain vulnerabilities are considered out of scope for our Responsible Disclosure Program, including physical testing of premises, social engineering, phishing, denial of service attacks, and resource exhaustion attacks.

Contact

When you have any questions regarding our Responsible Disclosure Policy please send an e-mail to incidenten@wecanmarketing.nl.