REPORT A SECURITY VULNERABILITY

Coordinated Vulnerability Disclosure intake form

Use this form to report a suspected security vulnerability affecting an Ramtech product or service.
Please provide enough technical detail to support validation. Do not include passwords, private keys, personal data or production credentials.

1. Reporter details

Name *

Company / organisation

Email address *

Telephone (optional)

2. Product information

Product name *

Product family / model *
If unknown, attach a clear image of the product label.

Firmware / software / hardware version or build *

Serial number or installation reference (optional)

3. Vulnerability information

Vulnerability title *

Detailed description *
What did you observe, where was it found, and under which conditions?

Steps to reproduce
Include preconditions, tools and test environment. Do not submit harmful payloads.

Affected functionality / interface
For example: radio, network, configuration tool, mobile application, cloud service or update process.

4. Potential impact

■ Confidentiality	■ Integrity
■ Availability	■ Authenticity
■ Safety	■ Privacy
■ Malicious code execution	■ Unknown

Impact details *
Describe the credible effect on products, users, data or connected systems.

5. Exploitation and incident indicators

■ Active exploitation: Yes	■ Active exploitation: No
■ Active exploitation: Suspected	■ Active exploitation: Unknown

■ Security incident: Yes	■ Security incident: No
■ Security incident: Suspected	■ Security incident: Unknown

Evidence or observations
State what supports the selection above.

6. Mitigation and disclosure

Mitigation or workaround already applied
Include any temporary measure and its observed effect.

■ Not publicly disclosed	■ Limited disclosure
■ Publicly disclosed	■ Unknown

Disclosure reference / intended disclosure date (if applicable)

Sensitivity classification
For example: public, confidential, highly confidential.

7. Supporting evidence

Attachments / evidence list
Screenshots, relevant logs, packet captures or proof of concept. Remove personal data, credentials and unrelated confidential information.

8. Declaration and privacy acknowledgement

■ I confirm that the information is accurate to the best of my knowledge.

■ I acknowledge that the information will be processed for vulnerability assessment, remediation, disclosure and legal compliance.

Reporter signature / typed name

Date

For company use: Case ID _____ Received _____ Initial classification _____

Website deployment note: connect the online form only to an approved, access-controlled case-management workflow. Define retention, encryption, access, acknowledgement and escalation rules before publication.