

Report a security vulnerability

Coordinated Vulnerability Disclosure intake form

Use this form to report a suspected security vulnerability affecting an Orama 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

Select all that apply

☐ 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

No

Suspected

Unknown

Possible security incident

Yes

No

Suspected

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.

Disclosure status

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

Click the button to attach this completed form to a new email automatically. This needs Adobe Acrobat or the free Adobe Acrobat Reader. In other PDF viewers the button opens a blank email instead, so save the form and attach it yourself, together with any supporting evidence.

For Orama use

Case ID

Received

Initial classification