CUBERA

Coordinated Vulnerability Disclosure Policy

Cubera Solutions AG
General-Wille-Strasse 96
CH-8706 Feldmeilen
www.cubera.ch

1 Purpose

This policy describes how security researchers, customers and other third parties can report vulnerabilities in products and services of Cubera Solutions AG, and how Cubera handles and discloses them. Its goal is that vulnerabilities are fixed or mitigated before they become public, and that everyone who needs to act is informed in time. The policy follows ISO/IEC 29147 (vulnerability disclosure) and ISO/IEC 30111 (vulnerability handling) and supports ISO/IEC 27001:2022 Annex A 5.24–5.26 and 8.8. It is published so that anyone can rely on it.

2 Scope

This policy covers:

- software developed by Cubera, including software, apps and SDKs developed on behalf of customers;
- services and infrastructure operated by Cubera, including hosted applications and the websites and domains of Cubera.

Not covered:

- systems and services of third parties that Cubera uses but does not operate; please report these to the respective provider;
- systems operated by Cubera's customers, even if they run software developed by Cubera; testing these requires the customer's permission (Section 6.3);
- reports that concern only missing best-practice settings without a demonstrable security impact.

3 How to Report

Please report vulnerabilities by e-mail to **security@cubera.ch**. The address and this policy are also listed in the `security.txt` file at `https://www.cubera.ch/.well-known/security.txt`. Reports can be written in German or English.

A helpful report contains:

- the affected product, version, URL or component;
- a description of the vulnerability and its potential impact;
- the steps to reproduce it, and a proof of concept where available;
- how you would like to be contacted and credited.

If you need to send sensitive details, ask for an encrypted channel in your first message. Customers with a support agreement may also use the channels agreed in their contract.

4 What You Can Expect from Us

Step	Target
Acknowledgement of receipt	within 3 working days
Initial assessment (validity, severity) communicated to you	within 10 working days
Status updates until resolution	at least every 30 days, and on material progress
Notice when the vulnerability is fixed or mitigated	on completion

Cubera treats every report confidentially. Remediation is prioritised by severity, likelihood of exploitation and exposure, following Cubera's vulnerability management process. If a report is not accepted as a vulnerability, Cubera explains why.

5 Coordinated Disclosure

5.1 Disclosure timeline

We ask you not to disclose a vulnerability before it has been fixed or mitigated and the affected parties have had reasonable time to act. As a default, Cubera aims for disclosure no later than **90 days** after the report. The date can be moved earlier by mutual agreement once a fix is available, or extended by mutual agreement if remediation requires more time.

5.2 Software developed for customers

If a vulnerability affects software that Cubera develops for a customer, Cubera informs the customer confidentially and coordinates remediation and disclosure with them. Where the software is integrated into the customer's own products, the fix reaches end users only through the customer's releases; the disclosure timeline takes this into account. The customer may publish the advisory for its own product. Cubera shares your identity with the customer only with your consent.

5.3 Active exploitation

If a vulnerability is actively exploited, Cubera handles it as a security incident. Cubera may then inform affected customers and parties earlier than agreed, to protect them.

5.4 Third-party components

If the vulnerability lies in a third-party component used by Cubera, Cubera informs its maintainer or asks you to report it upstream, and coordinates the timeline with all parties involved.

5.5 Advisories and CVE identifiers

After remediation, Cubera or the affected customer publishes an advisory where users need to act or the vulnerability is of public interest. Where appropriate, a CVE identifier is requested.

6 Safe Harbour

6.1 Commitment

Cubera considers security research carried out in good faith and in line with this policy to be authorised. Cubera will not file a criminal complaint or pursue civil claims against you for such research. If a third party takes legal action against you for activities in line with this policy, Cubera will make it known that your activities were authorised.

6.2 Rules for research

To remain within this policy:

- access, copy, modify or delete no more data than is necessary to demonstrate the vulnerability;
- stop and report immediately if you encounter personal data, credentials or data of other customers, and do not keep such data;

- use only your own accounts and test data;
- do not carry out denial-of-service attacks, social engineering, phishing, physical attacks or spam;
- do not use the vulnerability beyond demonstrating it, in particular not to move to other systems;
- keep the vulnerability confidential until it has been disclosed in coordination with Cubera;
- comply with applicable law.

If you are unsure whether an activity is covered, ask us at security@cubera.ch before you start.

6.3 Limits

This safe harbour covers systems operated by Cubera. Cubera cannot authorise testing of systems operated by customers or other third parties; their own policies apply. Vulnerabilities in software developed by Cubera can always be reported under this policy, however they were found.

7 Recognition

Cubera does not offer financial rewards. With your consent, Cubera credits you by name in the advisory.

8 Responsibility

The Chief Information Security Officer (CISO) is responsible for this policy and for the handling of reports. Reports are registered and handled under Cubera's vulnerability management process; suspected exploitation follows the security incident process. The reporting address is monitored on working days by at least two persons.

9 Review

This policy is reviewed at least annually and on material change. The `security.txt` file is renewed before its expiry date.