

Coordinated Vulnerability Disclosure Policy

This policy defines how Axel S.r.l. receives, handles, and discloses security vulnerability reports for its products.

Reference: CRA Annex I, Part II, point 5.

Scope

This policy applies to all software products developed and distributed by Axel S.r.l., compliant with CRA requirements. It covers vulnerabilities discovered by external security researchers, customers, or other third parties, as well as vulnerabilities identified internally.

How to report a vulnerability

Vulnerability reports must be sent to:

`security@axelsw.it`

Reports may be submitted in Italian or English. Please include the following information to help us assess and reproduce the issue:

- Product name and version number (any relevant information to identify the product and its exact version).
- A description of the vulnerability and its potential impact.
- Steps to reproduce the vulnerability (example project, if available).
- Your contact details for follow-up communication.

Our commitments to reporters

- Acknowledgement: we will acknowledge receipt of your report within 2 business days.
- Report validation: keeping regular contact with the reporter, we'll try to replicate the issue in order to evaluate its severity. We cannot grant a timeline for this phase since report replicability depends on external information. This phase can end with a positive report validation or a report rejection.
- Remediation: in case of positive report validation, we will address vulnerabilities within the timelines defined in following table, based on CVSS severity:

Severity	CVSS score	Target remediation time
Critical	≥ 9.0	≤ 15 calendar days from confirmation. Out-of-band release if necessary.
High	7.0 – 8.9	≤ 30 calendar days from confirmation, or the next scheduled release.
Medium	4.0 – 6.9	≤ 60 calendar days from confirmation, or the next scheduled release.
Low	< 4.0	$\leq$ next scheduled release.

Coordinated disclosure timeline

Axel S.r.l. follows a coordinated disclosure model. We ask reporters to:

- Allow us the remediation period defined above before any public disclosure.
- Contact us at `security@axelsw.it` if the remediation period needs to be extended or if there is evidence of active exploitation, so that we can coordinate an accelerated response.

If we are unable to remediate within the agreed timeline, we will communicate this to the reporter with an updated estimate and the reason for the delay. In all cases, Axel S.r.l. will not take legal action against researchers who report vulnerabilities in good faith and in accordance with this policy.

Exclusions

The following activities are outside the scope of this policy and may be subject to legal consequences:

- Accessing user data or systems beyond what is necessary to demonstrate the vulnerability.
- Denial-of-service attacks against Axel infrastructure or customer systems.
- Social engineering or phishing of Axel employees or customers.
- Physical attacks against Axel premises or hardware.

Publication

This policy is publicly accessible at company website.