LEGAL

Security and Responsible Disclosure

Found a vulnerability? Tell us — we'll thank you. This is how to report it, what we do next, and the safe harbour we give researchers.

ON THIS PAGE

1. How to report
2. What is in scope
3. What happens next
4. Safe harbour
5. Supported versions
6. Rewards

Version: 1.0

Effective date: 11 October 2026

Last updated: 11 October 2026

The short version

- Found a vulnerability in Cotterpin, our licence service or this website? Email **security@cotterpin.io**.
- We acknowledge within 2 business days and aim to fix critical issues within 7 days.
- Good-faith research under this policy is welcome, and we will not pursue legal action against it.

1. How to report

Email **security@cotterpin.io**. Please do **not** report a vulnerability in a public issue or pull request, or through support. Include:

- what you found and where;
- how to reproduce it;
- the Cotterpin version (`cotterpin --version`), if it concerns the software;
- the impact you expect.

2. What is in scope

- The Cotterpin software, its gate packs and agent adapters, at the latest release.
- The Cotterpin licence service and its API.
- This

Out of sc s' CLIs and serv victim's unlocked

May we use Google Analytics cookies to count visits and see which pages help? Nothing is set unless you accept, and you can change your mind any time. Cookie Policy

3. What happens next

STAGE	TARGET
Acknowledge your report	2 business days
Initial assessment	5 business days
Fix — critical	7 days
Fix — high	30 days
Notify the authorities of an actively exploited vulnerability (EU Cyber Resilience Act)	within 24 hours

We keep you informed as we work, publish an advisory for every fixed vulnerability, and credit you publicly if you want to be credited.

4. Safe harbour

We will not pursue legal action against, or ask law enforcement to investigate, good-faith security research that:

- respects our users' privacy and data — you access only what you need to show the issue, never another customer's data, and delete anything you obtained once reported;
- avoids degrading the service — no denial of service, spam or brute force beyond what proves the point;
- gives us a reasonable chance to fix the issue before you disclose it publicly;
- does not involve extortion or demands.

Research under this policy is authorised use for the purposes of our Terms of Service and Acceptable Use Policy. If a third party takes legal action against you for research that followed this policy, we will make it known that your actions were authorised by us.

For the purposes of the Computer Misuse Act 1990 and similar laws, we authorise research that follows this policy on the systems listed as in scope, and only those. We cannot authorise testing of systems we do not own or control, such as Paddle's, our hosting providers' (Amazon Web Services and Microsoft Azure) or your model provider's: their own policies apply. If you are unsure whether something is covered, ask us at security@cotterpin.io before you start.

5. Supp

Until ver ed on
every up check a
downloa we
protect r

May we use Google Analytics cookies to count visits and see which pages help? Nothing is set unless you accept, and you can change your mind any time. Cookie Policy

6. Rewards

We do not run a paid bug bounty at present. We will thank you, and credit you if you wish.

May we use Google Analytics cookies to count visits and see which pages help? Nothing is set unless you accept, and you can change your mind any time. Cookie Policy