RESPONSIBLE DISCLOSURE POLICY

Adopted by the Board of Directors on November 24, 2026

WHO WE ARE AND WHY

The 256 Foundation (256F) is a 501(c)(3) nonprofit that builds and stewards open-source alternatives to closed layers of the Bitcoin mining ecosystem. Our 256 Red Team researches the security of mining firmware and software. We are white-hat researchers. We practice responsible disclosure in line with general industry best practice, and we act for the mining industry and the people who use its products. When disclosure drags on, users carry the risk without knowing it.

SCOPE

This policy covers vulnerabilities we find in mining firmware, software and pool services, open or closed source. Our own projects follow the same principles. We test only hardware and systems we own or are authorized to test, and we never exploit other people's live systems.

HOW WE DISCLOSE

We report each vulnerability privately to the vendor or maintainer first. We then give the vendor reasonable time to fix it before publishing, consistent with industry best practice for coordinated disclosure. We decide timing case by case, weighing factors such as:

- Severity and ease of exploitation
- Whether it is actively exploited
- How many users are affected
- Whether a fix or mitigation is available
- How likely others are to find the same issue
- How responsive the vendor has been
- Whether a fix was released silently or did not work
- Whether the product is still maintained

UNRESPONSIVE VENDORS

We try to reach vendors through more than one channel, and we may ask a neutral coordinator for help. If a vendor does not engage, we may publish after a reasonable time.

EXTENSIONS

We may give more time to a vendor that is working on a fix in good faith. Extensions are at our discretion and are never guaranteed.

NOTIFYING USERS

Where it helps them protect themselves, we may notify users of affected products, from individual miners to large operators, before we publish. We make reasonable efforts but cannot promise to reach everyone.

WHAT WE PUBLISH

- If the issue is fixed, we publish a full advisory that notes the vendor's fix.
- If the issue is not fixed, we publish a limited advisory covering affected versions, impact and mitigations, with no details that would let someone reproduce the exploit.
- We publish exploit details only after users have had a reasonable time to update, if at all.
- We may publish a summary of our contact attempts with the vendor.
- We may share a draft with the vendor to check facts, but vendors cannot block, delay or change publication.
- Our advisories stick to the facts.

INDEPENDENCE

The same rules apply to every vendor and user, including 256F funders and partners. Donations never buy a review, its outcome or special treatment.

ETHICS

We never ask for money or anything else in exchange for silence or delay. We never sell findings. A person verifies every AI-assisted finding before it goes to a vendor.

REPORTING A VULNERABILITY TO US

Report vulnerabilities in 256F projects to security@256foundation.org. We will not pursue legal action against anyone who reports in good faith and follows this policy.

CVE IDENTIFIERS

We may request CVE IDs where useful.

GOVERNANCE

The Board of Directors adopts this policy. The Executive Director applies it case by case, and the board reviews it periodically.