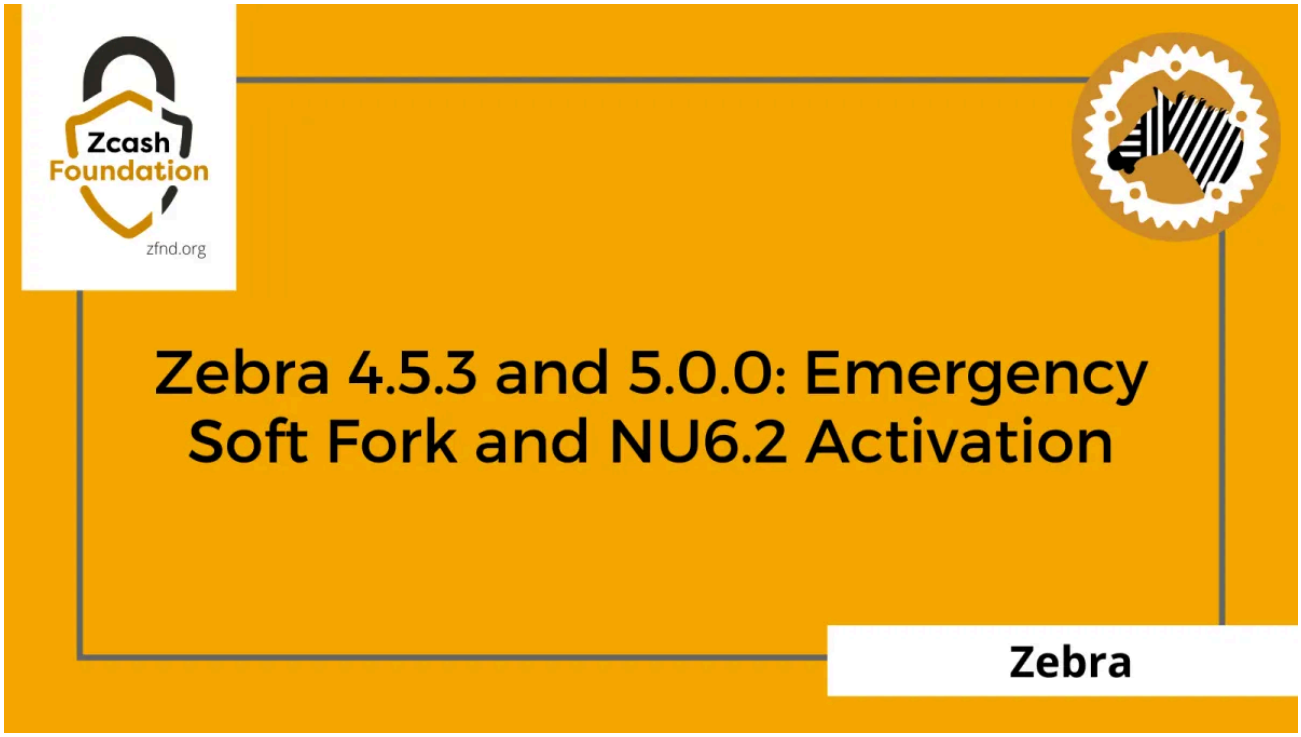
June 3, 2026 Foundation News

Zebra 4.5.3 and 5.0.0: Emergency Soft Fork and NU6.2 Activation



We have recently released **Zebra 4.5.3** and **Zebra 5.0.0**. These two releases work together to address a critical bug in the Orchard Action circuit: 4.5.3 implemented an emergency soft fork that temporarily disabled Orchard actions while the fix was being prepared, and 5.0.0 activated NU6.2, which re-enables Orchard using the corrected circuit.

We strongly urge all node operators to upgrade to Zebra 5.0.0 as soon as possible, or to 4.5.3 if you are unable to upgrade to 5.0.0 before the NU6.2 activation height.

What happened

On Friday, May 29, Taylor Hornby — an independent security researcher conducting an ongoing protocol audit on behalf of Shielded Labs — discovered a critical soundness vulnerability in the Orchard zero-knowledge proof circuit. Taylor responsibly disclosed the issue to ZODL core engineers that evening.

Within hours, ZODL engineers Daira-Emma Hopwood, Kris Nuttycombe, and Jack Grigg confirmed the issue and began evaluating remediation options. Over the following days, engineers, infrastructure operators, miners, and other ecosystem participants worked together to prepare a coordinated upgrade, all while keeping details of the flaw private to minimize the risk of exploitation before a fix could be deployed.

Private coordination with miners and exchanges began on the evening of Sunday, May 31. A first soft-fork activation attempt encountered coordination challenges during patch deployment; ZODL engineers quickly produced a second patch targeting block height **3,363,426**, which successfully activated at approximately 02:00 UTC on June 2. This soft fork temporarily rejected all Orchard-containing transactions and blocks.

On Wednesday, June 3, at 00:05 EDT, the NU6.2 hard-fork network upgrade activated successfully, re-enabling Orchard with the corrected circuit. This was the second security-driven protocol upgrade in Zcash history since its launch in 2016.

The vulnerability was caught before any known exploitation occurred. There is no evidence of unauthorized value creation. Zcash's turnstile mechanism (which tracks the total ZEC balance across all value pools) confirmed that the total supply remained intact throughout. User privacy was not affected. Sapling and transparent transactions continued operating normally throughout the incident.

The Vulnerability

The issue was a **soundness bug** in the implementation of the Orchard zero-knowledge proof circuit in the `halo2_gadgets` crate.

In a protocol like Zcash, *soundness* means the system should only accept valid transactions and state transitions. A soundness vulnerability is one that could allow the system to accept something it should reject. In this case, successful exploitation could have allowed the Orchard pool to accept invalid state transitions, potentially permitting double-spending of funds within Orchard, though with no ability to inflate the total ZEC supply, which is protected by Zcash's turnstile mechanism.

Affected versions

This vulnerability affects:

- All versions of `halo2_gadgets` prior to v0.5.0
- All versions of `orchard` prior to v0.14.0
- All versions of `zcash_primitives` prior to v0.28.0
- `zcashd` v5.0.0–v6.12.3
- `zebrad` versions below v4.5.1 (all earlier releases)

Zebra 4.5.3: Emergency Soft Fork

Zebra 4.5.3 implements the soft fork that temporarily disables Orchard actions. After the activation height, nodes reject any transaction or block containing Orchard actions. To preserve network connectivity during the upgrade window, 4.5.3 does not increase the DoS score of peers that continue to relay Orchard-containing blocks or transactions.

A direct patch would have revealed too much about the nature of the flaw to anyone with access to the updated code. Disabling Orchard as a first step limited the disclosure of vulnerability details while the circuit fix was finalized.

Security

- **GHSA-jfw5-j458-pfv6** (https://github.com/ZcashFoundation/zebra/security/advisories/GHSA-jfw5-j458-pfv6) (Critical): Temporarily disables Orchard actions via soft fork at height 3,363,426 on Mainnet to mitigate a critical soundness bug in the Orchard Action circuit. Orchard is re-enabled in the follow-on NU6.2 upgrade in Zebra 5.0.0.

Changed

- Set the soft-fork activation height for Orchard-disabling to block height 3,363,426 on Mainnet.
- Nodes running 4.5.3 do not penalize peers for relaying Orchard-containing data during the interim window.

Upgrading

Node operators who cannot immediately move to Zebra 5.0.0 should upgrade to 4.5.3 to stay on the correct chain. You can find the release on GitHub (https://github.com/ZcashFoundation/zebra/releases/tag/v4.5.3).

Zebra 5.0.0: NU6.2 Network Upgrade

Zebra 5.0.0 activates the **NU6.2 network upgrade**, which re-enables Orchard actions using the corrected circuit and permanently closes the vulnerability addressed by the 4.5.3 soft fork. A hard fork was required because remediating a zero-knowledge proof circuit bug requires updating the pinned verifying key, a change that cannot be made through a node software patch alone.

NU6.2 activates at:

- **Mainnet**: block height **3,364,600**
- **Testnet**: block height **4,052,000**

We recommend all node operators upgrade before the mainnet activation height. If the activation height has already passed and your node followed a fork, you will need to sync from scratch, or from a backed-up state taken before the activation height.

Added

- Activate the NU6.2 network upgrade (consensus branch ID `0x5437f330`) at height 3,364,600 on Mainnet and 4,052,000 on Testnet. NU6.2 re-enables Orchard actions with the fixed Orchard Action circuit and routes Orchard proofs to a per-circuit verifying key (`InsecurePreNu6_2 / FixedPostNu6_2`).
- Advertise network protocol version 170150 for NU6.2 on Mainnet, Testnet, and Regtest.

Changed

- Set the default Testnet temporary Orchard-disabling soft-fork height to 4,048,500; the disable window runs until NU6.2 re-enables Orchard actions at height 4,052,000.

Security

- **GHSA-jfw5-j458-pfv6** (https://github.com/ZcashFoundation/zebra/security/advisories/GHSA-jfw5-j458-pfv6): Add a consensus rule that rejects Orchard bundles whose proof has a non-canonical size, effective from the NU6.2 activation height. This permanently closes the vulnerability that the 4.5.3 soft fork mitigated.

Upgrading

We strongly recommend all Zebra node operators upgrade to 5.0.0 before block height 3,364,600 on Mainnet. Upgrading is the only way to ensure your node follows the correct chain after NU6.2 activates. You can find the release on GitHub (https://github.com/ZcashFoundation/zebra/releases/tag/v5.0.0).

Why the Orchard pool matters

The Orchard shielded pool is the centerpiece of Zcash's privacy architecture, introduced with NU5 in 2022. Built on the Halo 2 proving system, it is the first Zcash pool to require no trusted setup, a long-standing goal for the ecosystem. Over the past year it has grown significantly, and today holds a substantial fraction of circulating ZEC.

Zcash's turnstile mechanism, which tracks the total ZEC balance across all value pools (Sprout, Sapling, Orchard, transparent, and lockbox) and enforces invariants on how much value can flow between them, was an important part of what made this incident manageable. It provided a ground truth that ecosystem participants could use to confirm the supply cap remained intact, even while the Orchard circuit fix was being developed.

Coordinated response

This upgrade succeeded because the necessary pieces were already in place: ongoing security review by independent researchers, established responsible disclosure procedures, experienced protocol engineers, and a network of independent participants who acted quickly when required.

ZODL developed the remediation and led coordination, but the upgrade required voluntary cooperation from miners, node operators, infrastructure operators, exchanges, wallet providers, and other network participants, all acting independently around a shared goal of protecting users and preserving the integrity of the network.

Unlike contentious forks sometimes seen across the industry, this was a security response. The issue was discovered, responsibly disclosed, confirmed, remediated, and resolved in a few days. We are proud of how the ecosystem came together.

Acknowledgments

The Zcash Foundation extends its sincere thanks to **Taylor Hornby** for discovering and responsibly disclosing this vulnerability, and to Shielded Labs for supporting the independent security research that made it possible.

We are grateful to the ZODL engineers whose deep protocol expertise made a rapid remediation possible, in particular **Jack Grigg**, **Daira-Emma Hopwood**, and **Kris Nuttycombe**.

Special recognition goes to **Arya Solhi** of the Zcash Foundation, who was instrumental in developing the Zebra patches that enabled the network upgrade.