MultiversX mainnet · 19 to 24 September 2026

MultiversX Post-Mortem Incident Report

CONTENTS

1	Summary	3
2	Timeline	4
3	Root cause	6
4	Impact	9
5	Response and recovery	11
6	Recovery milestones and corrective actions	14
	Closing note	15
	References	16
A	Evidence and verification	16

KEY FACTS

Status	Block production resumed on 24 September 2026 after the checkpoint recovery and the deployment of both fixes. Our checks on 29 September confirmed the checkpoint and the exclusion of the exploit transactions. The bridge to Ethereum reopened on 25 September and carried no illegitimate transfer. We have completed our reconciliation with the exchanges and consider the matter closed on our side.
What happened	A multi-asset transfer failed partway: the recipient's credits had been saved, the sender's debit had not, and the VM hook reported the failure to the calling contract without undoing it. Repeated, the gap doubled the credit with each of the first 30 calls.
Root cause	Two defects, both required, both fixed. **F-1**: MultiESDTNFTTransfer saved the recipient's credits before a step that could still fail (mx-chain-vm-common-go). **F-2**: the hook returned failure without restoring state (mx-chain-vm-go).
Invalid state	76,679,661.700615 EGLD, seven bridged token balances multiplied by 2^{31}, and 31 copies of a single-supply NFT, created in 55 minutes. None of it exists on the recovered chain.
Containment	Validators halted block production; the last block passed consensus at about 07:41 UTC, roughly an hour after the first exploit call. Exchanges blocked or declined the exploit-derived deposits. MEXC credited one; it sits on MEXC's own ledger and is for MEXC to resolve. The Poloniex matter is closed and resolved. Bridge paths were paused, and we engaged law enforcement.
Recovery	A hard fork from round 33,384,826, the last round before the first exploit call, removed about an hour of blocks and activated the fixes. We resubmitted the legitimate transactions from that hour after the restart and gave the all-clear on 24 September at 15:53 UTC.

1 Summary

> **Status.** Block production resumed on MultiversX mainnet on 24 September 2026, after the checkpoint recovery and the deployment of fixes for both VM defects. Our checks against the recovered chain on 29 September confirmed the checkpoint and the exclusion of the exploit transactions (section 5.6). The exploit contract held its pre-exploit asset balances, and the operator account held no copy of the duplicated NFT. We resubmitted the legitimate transactions from the removed hour, and most completed. The bridge to Ethereum reopened on 25 September, and our engineers confirmed that no illegitimate transfer passed through it. Section 4.2 describes the financial outcomes.

At 06:37:45 UTC on Saturday 19 September 2026, an attacker began creating assets on MultiversX mainnet without an authorised minting operation. Over the next 55 minutes, 31 calls to a single contract produced 76,679,661.700615 EGLD in invalid credits, multiplied the balances of seven bridged tokens by 2^{31}, and made 31 copies of an NFT that should exist once.

The attack relied on a transfer that failed partway and was never undone. The attacker's contract, written by hand in WASM, called a fallible VM hook with a multi-asset transfer that ended with an NFT. The built-in function performing the transfer saved the recipient's credits and then failed at a later step, building the output for the NFT transfer, before the sender's debit was saved. The hook reported the failure to the contract without restoring state, the contract ignored the returned error status, and the transaction completed. The recipient retained the credited assets, while the sender's persisted balance was not reduced. Sending the assets back doubled the contract's balance. The attacker made 31 calls in all, sending the credit back after each of the first 29.

Validator operators halted block production following an urgent request, each stopping their own nodes. The last block passed consensus at about 07:41, roughly an hour after the first call and about nine minutes after the last. Most exchanges blocked or did not credit the exploit-derived deposits, bridge paths were paused, and we engaged law enforcement. We had a fix ready for validation the same day. We rehearsed the recovery on an internal testnet on the night of 20 September, then on the public Testnet, and with validators on Devnet on 22 September. On 23 September a coordinated hard fork activated the fixes and restarted the chain from round 33,384,826, the last round before the first exploit call. The hard fork completed, but Shard 1 repeatedly failed to reach consensus, and we asked validators to stop again so that more Shard 1 nodes could synchronise. Production resumed the next day on v2.1.5, and we gave the all-clear at 15:53 UTC on 24 September.

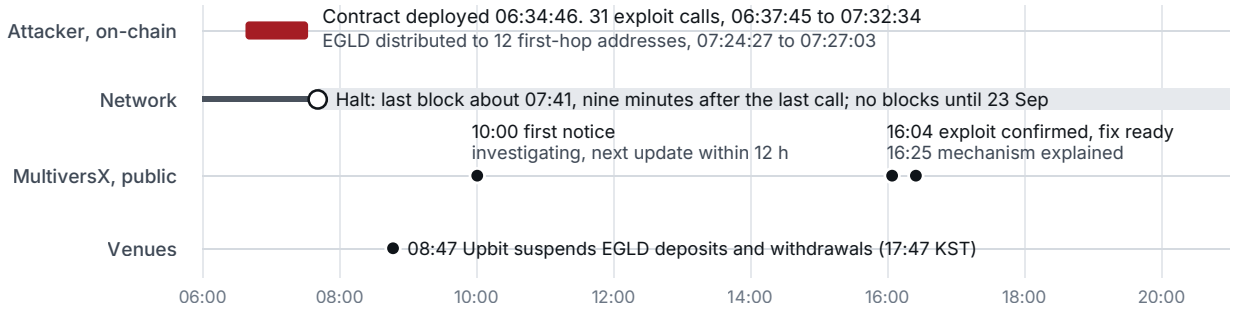
Account balances on MultiversX were restored to their state immediately before the exploit. The recovery removed about an hour of blocks, from the first exploit call to the halt, and we resubmitted the legitimate transactions they contained. Apart from the restart on 23 September, the network produced no blocks for five days. Off-chain, MEXC credited one deposit, and any position it left is for MEXC to resolve. The Poloniex matter is closed and resolved, and our reconciliation with the exchanges is complete.

Section 6 sets out the recovery milestones and the corrective actions we have taken.

2 Timeline

All times are UTC. The attack ran for 55 minutes on the morning of Saturday 19 September, and the chain halted about nine minutes after the last exploit call. The network returned to normal operation on the afternoon of Thursday 24 September; services and exchanges followed over the next days.

a) Saturday 19 September, 06:00 to 21:00 UTC



b) 16 to 25 September, UTC

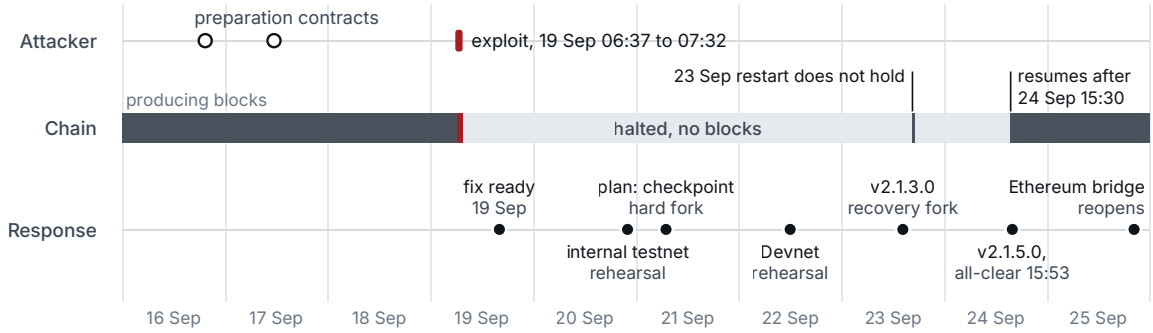


Figure 1. Incident timeline. (a) The first day: the halt came about nine minutes after the last exploit call. (b) 16 to 25 September: no block production from the halt until 24 September, apart from the restart on 23 September.

UTC	EVENT
PREPARATION AND EXPLOIT	
16 and 17 Sep	The operator account deploys two preparation contracts, at 19:20 on 16 September and 11:23 on 17 September.
19 Sep 06:34:46	The operator deploys the exploit contract and, by 06:35:39, seeds it with 0.047609 EGLD, seven bridged tokens and a newly created NFT.
06:37:45	**First exploit call.**
06:37:45 to 07:19:15	Calls 1 to 30. The EGLD credited per call doubles each time, from 0.047609 to 25,559,887.249408.
07:24:27 to 07:27:03	9,812,375.77 EGLD sent to 12 first-hop addresses.
07:32:34	**Call 31, the last,** repeats the largest amount.
HALT AND FIRST RESPONSE	
About 07:41	**Halt.** The last block passes consensus. Validator operators have stopped their nodes following an urgent request in the validator channel, and the shards fall quiet one after another.
08:47	Upbit suspends EGLD deposits and withdrawals.
10:00:49	We publish our first public notice: a potential mainnet issue is under investigation, with an update to follow within 12 hours.

UTC	EVENT
16:04:11	We confirm the exploit of a VM-level atomicity issue. The network stays paused, and a fix is ready for validation.
16:25	One of our core developers explains the mechanism publicly.
20 Sep	Our public update confirms that the attacker's accounts had already been identified and frozen with major exchanges, and that law enforcement had been engaged. One of our core developers adds that the fixes span both VM repositories.
RECOVERY	
21 Sep 07:00	We publish the recovery plan: a coordinated hard fork from a known-good checkpoint, to be rehearsed on Testnet and Devnet.
10:32	Our engineers report a successful hard-fork rehearsal on an internal testnet the previous night and prepare mainnet checkpoints.
22 Sep	We rehearse the recovery with validators on Devnet, after a rehearsal on the public Testnet.
23 Sep 14:19	We publish the recovery release: mainnet-config v2.1.3.0 and mx-chain-go v2.1.3, carrying the checkpoint, the round exclusions and the fixes.
16:35	The chain resumes from the checkpoint and the hard fork completes, but Shard 1 repeatedly fails to reach consensus.
17:13	We ask validators to stop their nodes, so that more Shard 1 nodes can synchronise and a backlog does not build. At 19:22 we announce that the chain will stay paused overnight while we plan a longer upgrade window and test across the epoch transition.
24 Sep 11:08	We announce v2.1.5.0, with synchronisation improvements. The logs show the hard fork need not be repeated.
After 15:30	Block production resumes.
15:53	**All-clear.** We confirm the network is ready for normal activity.
SERVICE RESTORATION	
25 Sep	xExchange is back to normal operation. The bridge to Ethereum resumes processing after its own readiness checks, and we announce its reopening at 20:22.
27 Sep	Web Wallet confirmed working normally: login, transaction signing, balance and transaction displays.
28 Sep	Public nodes and gateway confirmed operational.
29 Sep 17:42	We release mx-chain-go v2.1.7. Its API filters records from the excluded rounds on nodes that run it, and it hardens a separate VM execution path; neither change is part of the incident fix.
30 Sep	Binance.US confirmed to have EGLD deposits and withdrawals enabled.

3 Root cause

3.1 The property that broke

A fallible operation makes its caller one promise: if it reports failure, nothing happened, apart from the gas it consumed and the record of the failure.

$$\text{fallible operation reports failure} \Rightarrow \text{state}_{\text{after}} = \text{state}_{\text{before}}$$

State here means everything the operation could touch: balances, token quantities and metadata, output transfers, logs, storage and journals. Asset conservation follows from it. For every asset a, summed over all accounts:

$$\Sigma\ \text{balance}_{\text{after}}(a) = \Sigma\ \text{balance}_{\text{before}}(a) + \text{mint}(a) - \text{burn}(a)$$

where mint and burn are authorised issuance and destruction, both zero for an ordinary transfer. On 19 September the first property failed, and the second failed through it.

3.2 Finding F-1

F-1

MultiESDTNFTTransfer saved the recipient's credits before a step that could still fail

Component	mx-chain-vm-common-go, `builtInFunctions/multiESDTNFTTransfer.go`; blockchain hook `ExecuteBuiltInFunction` and `ProcessBuiltInFunction`
Severity	Critical in combination with F-2
Status	**Fixed.** Active on mainnet since the recovery hard fork of 23 September.

MultiESDTNFTTransfer credited the recipient with every leg of the transfer and saved the recipient's account before it had finished building the outputs for the NFT transfer, a later step that could still fail. The sender's account was saved only once the built-in had returned successfully.

When that later step failed, the function returned an error before the sender's debit was saved. The debit existed only in memory and was discarded. The recipient gained, the sender lost nothing, and no mint had run.

3.3 Finding F-2

F-2

The fallible multi-transfer hook returned failure without restoring state to the pre-transfer snapshot

Component	mx-chain-vm-go, `managedMultiTransferESDTNFTExecuteWithReturn` in `vmhost/vmhooks/managedei.go` and `baseOps.go`. Added in Barnard (node v1.10.4, VM v1.5.43) behind the Barnard opcode flag and active on mainnet from epoch 1820, scheduled for 24 July 2025 at about 17:00 UTC. Introduced in VM v1.5.43; v1.5.49 confirmed affected.
Severity	Critical in combination with F-1. On its own it still breaks failure atomicity.
Exploitability	No privileges needed: a contract that ignores the returned status, and a transfer that fails after the built-in has already saved the recipient.
Status	**Fixed.** Active on mainnet since the recovery hard fork of 23 September.

Called with `withFailure = false`, the hook does not abort the execution. It returns status 1 and leaves the calling contract to decide what to do. It takes a snapshot before the transfer, but on this error path it returned without restoring the state the built-in had already changed.

```
managedMultiTransferESDTNFTExecuteWithReturn
  → TransferESDTNFTExecuteWithTypedArgsWithFailure(..., withFailure = false)
      snapshotBeforeTransfer = host.Blockchain().GetSnapshot()
      output.TransferESDT(...)   // → ProcessBuiltInFunction → MultiESDTNFTTransfer
      // the built-in fails after the recipient was saved
      return 1                   // no RevertToSnapshot(snapshotBeforeTransfer)
```

A later branch of the same function, for failures during destination execution, does call `RevertToSnapshot`. The rollback was intended; this path missed it.

3.4 How the defects combined

Neither defect could create assets on its own. The built-in was safe if its caller rolled back on error; the hook was safe if the built-in was atomic. Each relied on a guarantee the other did not give. Figure 2 follows one call.

STEP	WHERE	WHAT HAPPENS	CONTRACT	OPERATOR
1	Contract	Calls the hook: send its x EGLD, its balance of each of 7 bridged ESDTs and, last, one NFT with large metadata to the operator. Forwarded gas leaves the final step short. `withFailure = false`	x **saved**	b **saved**
2	VM hook	Takes a snapshot of state before the transfer. `S = host.Blockchain().GetSnapshot()`	x	b
3	Built-in	Credits the operator with every leg, the EGLD, the ESDTs and the NFT, and saves the operator's account. `accounts.SaveAccount(acntDst)`	x *debit in memory*	b + x **saved, +1 NFT**
4	Built-in	Then builds the output for the NFT transfer. This later step fails.	x	b + x
5	Built-in	Returns an error before the sender's debit is saved, so the debit is dropped. F-1	x **debit dropped**	b + x
6	VM hook	Returns status 1 to the contract. The state is never restored. F-2 `RevertToSnapshot(S) // never called`	x	b + x **kept**
7	Contract	Ignores the status and returns normally. The transaction succeeds and its state commits.	x	b + x **x created**
8	Operator	Next transaction: sends x back to the contract.	2x **doubled**	b

Repeated 31 times. The EGLD credit went back to the contract after each of the first 29 calls; the operator kept calls 30 and 31. Each ESDT seed ended at 2^{31} times its size, and the operator received 31 copies of the NFT.
x = contract balance at the start of a call; b = operator balance.

Figure 2. State changes during one exploit call. Steps 1 to 7 happen inside one exploit transaction; step 8 is the next transaction. Shaded rows mark the two defects. The right-hand columns show the saved balances of the contract (x) and the operator (b) after each step. Both accounts are in Shard 0, so the built-in credited the operator directly within each call.

The attacker's contract was built for this path. It was hand-written WASM rather than SDK output. It placed an NFT with large metadata last in a transfer of EGLD and seven fungible tokens (ESDTs, the MultiversX token standard), and forwarded gas that left the final step short. It was deployed from the operator account's nonce 19, after two preparation contracts on 16 and 17 September, and the first successful call came 2 minutes 59 seconds after deployment.

3.5 What was ruled out

No authorised mint ran: none of the 31 calls incremented the metachain's supply accounting or the registered token supply counters, while account balances grew. Nor was it a consensus failure: validators agreed on every block, and the fault lay in what those blocks executed. The defect was not confined to one contract, since any contract that ignored the hook's failure status could have committed partial state. We ruled out asynchronous execution publicly on 20 September, and the vulnerable hook had been on mainnet since Barnard in July 2025, so this was not a regression from the Supernova upgrade of 10 September.

4 Impact

4.1 Invalid state created

The figures in this section describe the chain before recovery and come from our initial reconstruction of the exploit transactions; Appendix A checks their arithmetic. None of these balances exists on the recovered chain.

ASSET	INVALID STATE	HOW IT AROSE
EGLD	76,679,661.700615 EGLD credited without a matching debit	30 calls doubling from 0.047609 EGLD, then one repeat of the largest amount

Seven bridged tokens
`BSCUSDC-887875`
`BSCUSDT-059796`
`BSCTADA-f64757`
`ETHWBTC-74e282`
`ETHWETH-e1c126`
`ETHUTK-8cdf7a`
`ETHUSDC-220753`
	Each balance on the exploit contract ended at its seed × 2^{31}	31 doublings of the seeded amount

NFT `TK31266898-70757d-01`	31 copies on the operator account; the original stayed on the contract	Registered supply is one

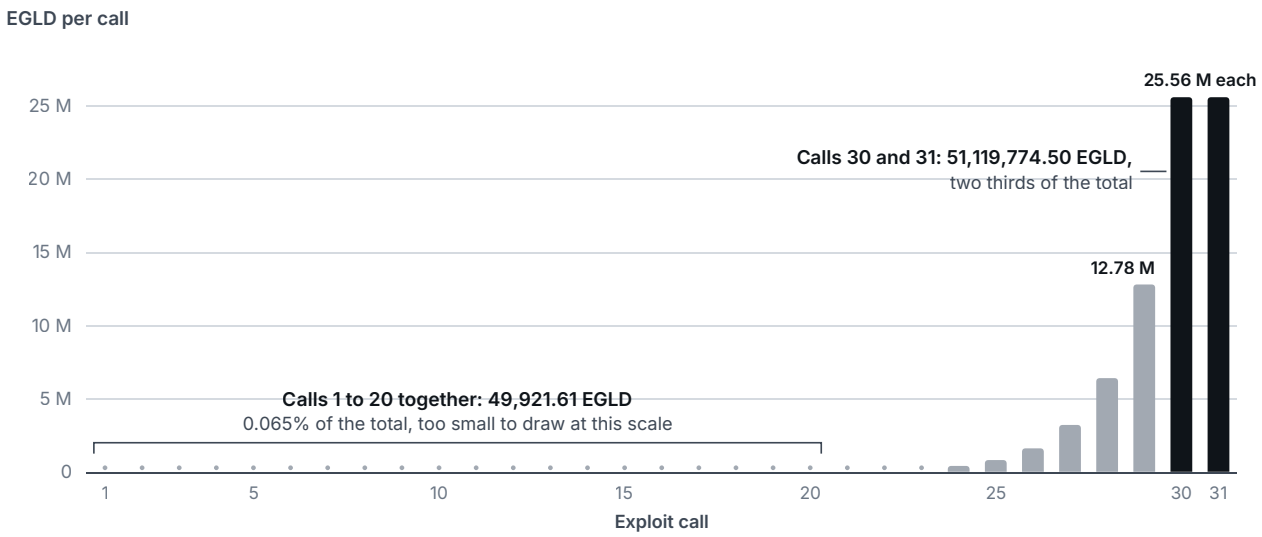


Figure 3. Invalid EGLD credited per exploit call. Linear scale. The first call credited 0.047609 EGLD and each later call doubled the one before, up to call 30; call 31 repeated call 30.

4.2 Where the value went

The contract ended with 25,559,887.249408 EGLD: its seed plus the credits from calls 1 to 29, which the operator sent back to it. The operator kept the 51,119,774.50 EGLD credited by calls 30 and 31, and between 07:24:27 and 07:27:03 sent 9,812,375.77 EGLD of it to 12 first-hop addresses. The balances remained at three of those addresses, 2,542,477.50 EGLD in total. The other nine forwarded most of theirs to exchange deposit addresses, and by 23 September we had mapped every one of those addresses to its exchange. Receiving these funds does not make the exchanges or their customers participants.

The exchanges' own reports establish what happened to the deposits:

EXCHANGE	REPORTED OUTCOME
HTX	Risk controls stopped the deposits from being credited; nothing was sold or transferred on HTX.
Kraken	Deposit not credited; funding operations suspended.
Bybit	Two previously unidentified addresses attributed to Bybit; deposit unsuccessful.
Binance, Coinbase	Deposits suspended during the incident period.
Upbit	No deposits or withdrawals during the period.
Poloniex	Address attribution confirmed; matter closed and resolved.
MEXC	Deposit credited; any resulting ledger position is for MEXC to resolve under its own processes.

MEXC credited one exploit-related deposit. Whatever position that left on its ledger is for MEXC to resolve, under its own processes and in its own time; it has no effect on MultiversX balances, which the recovery restored to their pre-exploit state. Poloniex confirmed the attribution of the deposit address, and that matter is closed and resolved. Our reconciliation with the exchanges is complete, and on our side the loop is closed.

At the end of the reconstructed exploit sequence, the seven bridged-token balances on the exploit contract each stood at their seed balance multiplied by 2^{31}. Our engineers confirmed that no illegitimate transfer passed through the bridge to Ethereum. The NFT copies remained on the operator account.

4.3 Effect on users and services

- **Five days without block production,** from the halt at about 07:41 on 19 September until 24 September, apart from the restart on 23 September.
- **Transactions in the removed hour.** Blocks produced between 06:37:45.6 and approximately 07:41 UTC on 19 September are not part of the recovered chain. After the restart, we resubmitted every legitimate transaction from those blocks that could be replayed, excluding the attacker's activity. Most completed. Some failed because their logic no longer applied after the pause. None of the failed resubmissions involved the bridge.
- **Staking.** Native staking rewards were not generated during intervals without block production. Rewards for the two elapsed epochs were distributed on 24 September, and the latest distribution was reported correct on 25 September.
- **Exchanges and the bridge.** Exchanges paused EGLD deposits and withdrawals during the incident. EGLD deposits and withdrawals were confirmed open at Binance.US on 30 September and at Binance on 9 October, and XT announced their resumption on 13 October. The bridge to Ethereum resumed processing on 25 September.

5 Response and recovery

5.1 Containment

The halt had two purposes: to stop new transactions from building on invalid state, and to stop anyone, the attacker or an imitator, from calling the hook again. Validator operators stopped their nodes after an urgent request in the validator channel; by their account, each decided individually. The shards fell quiet one after another, and the last block passed consensus at about 07:41, shortly after the final exploit call at 07:32:34. A shard stops once too few of its validators sign to reach consensus, so the halt needed enough operators in every shard rather than all of them.

Alongside the halt:

- We asked users not to submit or rebroadcast transactions, and not to move EGLD or tokens through exchanges or bridges until a separate all-clear.
- We paused bridge issuance, redemption and withdrawal for the affected tokens until custody and supply could be reconciled.
- We sent the attacker's addresses to exchanges, and most blocked or declined the exploit-derived deposits (section 4.2). Our exchange coordination team handled venue contact, our legal team handled incident submissions and counterpart requests, and we engaged law enforcement.
- Before any state was rewritten, we preserved archive databases, trie storage, transaction data, contract bytecode, logs and node binaries.

5.2 The fix

Both properties in section 3.1 were already rules of the protocol; on one path, the built-in function and the VM hook broke them. Our fix brings that path back into line at three layers:

- **Transfer built-in** (mx-chain-vm-common-go): the recipient's account is saved only after the fallible output-construction work.
- **VM** (mx-chain-vm-go): account snapshots and execution-output state are restored when the transfer or destination execution fails.
- **Node integration:** snapshot restoration also covers built-in execution and account-save failures.

In outline, the VM change on the transfer error path:

```
gasLimitForExec, executeErr := output.TransferESDT(transfersArgs, contractCallInput)
if executeErr != nil {
    host.Blockchain().RevertToSnapshot(snapshotBeforeTransfer)
    if withFailure {
        FailExecution(host, executeErr)
    }
    return 1
}
```

The corrective dependencies and node rollback handling were already in v2.1.0 and carried into the v2.1.3 and v2.1.5 recovery builds, and the recovery hard fork activated them on mainnet on 23 September. Each change went through an initial code review, a second review after revisions, and a final review by our VM lead.

The v2.1.7 release of mx-chain-go, published on 29 September, pins the corrected modules to tagged versions: mx-chain-vm-go v1.5.51 and mx-chain-vm-common-go v1.7.2. It also hardens a separate VM execution path and keeps records from the excluded rounds out of its API; neither change is part of the incident fix.

5.3 Choosing the recovery

We needed a recovery that would remove every invalid credit and leave legitimate state intact. A surgical migration would have kept every block after the exploit and deleted the invalid balances one by one, preserving legitimate activity in that window, but it would have depended on an exact list of invalid fields inside accounts that also held legitimate value, and on a new mechanism that outsiders could not easily check. A deeper rewind, or wholesale replacement of the affected accounts, would have destroyed more legitimate history.

We chose a checkpoint hard fork: restart from the last round before the first exploit call, exclude the exploit-era rounds, and activate the fixes in the same fork. It removes invalid state by construction, without having to find every invalid field, and anyone can verify it against the published header hashes. Its price was the hour of legitimate activity in the removed blocks, which we resubmitted after the restart.

5.4 Recovery parameters

PARAMETER	VALUE
Checkpoint round	33,384,826, starting 19 September 2026 at 06:37:45.0 UTC
Metachain header hash	`1f036cc21c9cb9fde00bad869666d9dd9c6b12278b55df5e07ce67c4db8e41a6`
Shard 0 header hash	`8c5b2e8a75ce938960b63503d98b88ca670286cb4cf60d16088ea6a7dae9f1a2`
Shard 1 header hash	`48a9fb558d27902d96bd4e8a09c1efab5e9231f98662068b95240943595cf850`
Shard 2 header hash	`a0b6f4347a26b90599ae64a7ac910d87df4b55a1992611df3a57b63e65c3593c`
First excluded window	Rounds 33,384,827 to 34,020,551 (19 Sep 06:37:45.6 to 23 Sep 16:35): the rolled-back hour, then the halt up to the coordinated restart
Second excluded window	Rounds 34,047,051 to 34,158,051 (23 Sep 21:00 to 24 Sep 15:30): the pause before block production resumed on 24 September
Blocks actually removed	19 Sep from 06:37:45.6 to about 07:41; the rest of the first window held no blocks
Releases	mainnet-config v2.1.3.0 and mx-chain-go v2.1.3 (recovery hard fork); v2.1.5.0 (restart)

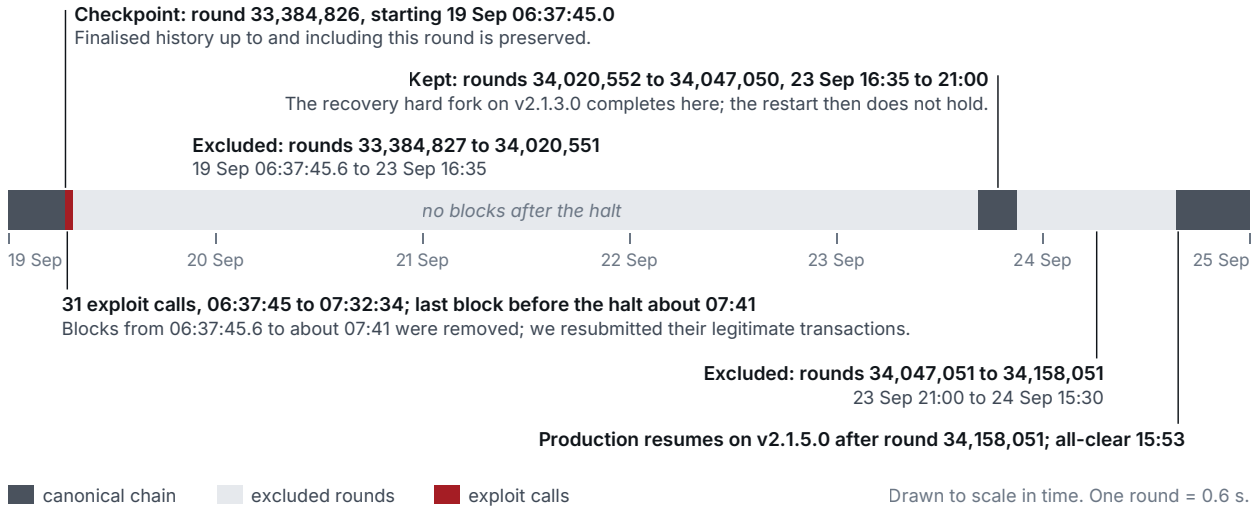


Figure 4. Recovery checkpoint and excluded rounds. Both windows are published in mainnet-config. The first runs from the rolled-back hour to the coordinated restart on 23 September, and only its first hour held blocks; the second covers the pause before production resumed on 24 September. Times follow from 0.6-second rounds and match block timestamps on the live chain.

5.5 Restart

23 September. We published the recovery release at 14:19, and the chain resumed from the checkpoint at 16:35. The hard fork completed, including the metachain's confirmation of Shard 1 blocks, but Shard 1 repeatedly failed to reach consensus. At 17:13 we asked validators to stop their nodes, so that more Shard 1 nodes could synchronise and a backlog would not build. At 19:22 we announced that the chain would stay paused overnight while we planned a longer upgrade and synchronisation window for the next day and tested across the epoch transition.

24 September. At 11:08 we announced v2.1.5.0, which improved synchronisation. Completing the hard fork and restoring stable block production were separate milestones: the hard fork had completed the day before, so this restart restored sustained consensus and did not rewrite state again. Block production resumed after 15:30. The upgrade window took about four and a half hours, shorter than the 8 to 12 hours we had announced the evening before. We gave the all-clear at 15:53 against three criteria: recovery upgrade deployed, block production resumed, and engineering recovery checks complete. We then resubmitted the legitimate transactions from the removed hour (section 4.3).

5.6 Verifying the recovered chain

Anyone can repeat the checks that matter against the public API. We ran them for this report on 29 September 2026.

1. **The checkpoint is canonical.** The four published header hashes are the blocks at round 33,384,826 in the metachain and in each shard, all timestamped 06:37:45.000.
2. **The exploit rounds are excluded.** In Shard 0, where the attacker's accounts sit, the block after the checkpoint is at round 34,020,552, on 23 September at 16:35:00.6, and names the checkpoint block as its parent. The first exploit call, timestamped 06:37:45, fell in round 33,384,827, the first excluded round. The checkpoint round contains no exploit transaction, and any other use of the hook after the checkpoint was removed with the same rounds.
3. **The attacker's accounts hold only their own pre-exploit funds.** Neither the first nor the last exploit call exists on the live chain. The exploit contract holds exactly its seed: 0.047609 EGLD, its original balances of the seven bridged tokens, and the one original NFT. The operator account holds no copy of the NFT, and its history runs from its last transaction before the exploit, at 06:35:39, straight to new transfers on 27 September.

6 Recovery milestones and corrective actions

6.1 Recovery milestones

The recovery hard fork completed on 23 September and activated both incident fixes. Sustained block production resumed on 24 September on v2.1.5, and we gave the all-clear at 15:53 UTC. Our v2.1.7 release of 29 September added filtering of excluded-round API records and hardened a separate VM execution path; those changes were separate from the incident fix.

We checked the recovered state against the public API on 29 September, as documented in section 5.6 and Appendix A.3. We resubmitted the legitimate transactions from the removed hour that could be replayed; section 4.3 describes the residual outcomes.

The bridge to Ethereum reopened on 25 September after its readiness checks. Our engineers confirmed that no illegitimate transfer passed through it and that every legitimate transfer was served. Web Wallet was confirmed working normally on 27 September. Public nodes and the gateway were reported operational on 28 September, with further infrastructure confirmation on 29 September.

xExchange was reported back to normal operation on 25 September. Hatom reported normal lending and liquid staking with no affected users, and OneDex reported no issues at the time of its update.

EGLD deposits and withdrawals were confirmed open at Binance.US on 30 September and at Binance on 9 October, and XT announced their resumption on 13 October.

6.2 Corrective actions

The transfer built-in now saves the recipient account only after the fallible output-construction work. The VM restores account snapshots and execution-output state when the transfer or destination execution fails. Node integration also restores snapshots following built-in execution and account-save failures. We included these corrective changes in the recovery builds, and the 23 September recovery hard fork activated them on mainnet (section 5.2).

After the first restart, Shard 1 repeatedly failed to reach consensus. We asked validators to pause so that more nodes could synchronise, tested across the epoch transition, and used a longer upgrade and synchronisation window for the 24 September restart. That restart restored sustained block production without repeating the recovery hard fork (section 5.5).

Closing note

We fixed the VM defects and removed the exploit-derived state through checkpoint recovery. Sustained block production resumed on 24 September. The interruption kept users from transacting normally, and we had to resubmit the legitimate transactions from the removed hour. Our reconciliation with the exchanges is complete. The one deposit credited at MEXC is now a matter for MEXC to settle on its own books, in its own time.

This network was defended by people who chose to act. Validator operators made the call themselves and halted the chain fast, by rough consensus. Exchanges and independent partners acted quickly to freeze the attacker's funds. Our team had a fix on the first day and proceeded to test it thoroughly before going into production. Our community held the line and stood with us throughout.

The larger lesson outlasts this incident. Relentless security tooling, round-the-clock red-teaming and response at blitz speed are the new baseline, and we have spent months building them. Verifiably correct-by-construction software is moving, as we speak, from an academic ideal to an engineering imperative.

To the validators, the exchanges, our team and our community: a big, heartfelt thank you. We defended this network together, and we will keep defending it.

References

- Recovery node release: mx-chain-go v2.1.3
- Restart node release: mx-chain-go v2.1.5
- Recovery configuration: mainnet-config v2.1.3.0
- Restart configuration: mainnet-config v2.1.5.0
- Follow-up release, separate from the incident fix: mx-chain-go v2.1.7
- Origin of the fallible VM hooks: mx-chain-vm-go pull request #907 (Barnard)
- Corrected modules pinned by v2.1.7: mx-chain-vm-go v1.5.51 and mx-chain-vm-common-go v1.7.2
- Public notices on X, UTC: @MultiversX 19 Sep 10:00:49 and 16:04:11, 21 Sep 07:00, 25 Sep 20:22; @CodeMultiversX 21 Sep 19:04, 23 Sep 14:19 to 19:22, 24 Sep 11:08, 15:53 and 17:10; @SasuRobert 19 Sep 16:25, 20 Sep 13:02, 24 Sep; @beniaminmincu 20 Sep
- XT announcement on the resumption of EGLD deposits and withdrawals, 13 October 2026
- Context: Barnard activation at epoch 1820, scheduled for 24 July 2025 (MultiversX release notes); Supernova activation at epoch 2233 on 10 September 2026; Upbit's suspension at 17:47 KST, as reported by bitbase.com
- Technical verification data: Appendix A of this report, with the account identifiers, transaction hashes and checks run against api.multiversx.com on 29 September 2026

A Evidence and verification

A.1 Accounts and assets

ROLE	ADDRESS OR IDENTIFIER
Operator account Shard 0	`erd1kwvkch79edm9qtg3tlaylgm9yff04lr9vaszazuavxtqrffz6scqrvvjd2`
Exploit contract Shard 0; WASM; deployed at operator nonce 19	`erd1qqqqqqqqqqqqqpgqsqffm2ezs77zsu6cvc6nxd4v8qegne4v6scqke2kq9`
Attacker NFT Registered supply one	`TK31266898-70757d-01`

A.2 Key transactions

Transactions before the checkpoint are part of the recovered chain. Those after it exist only in the preserved pre-recovery archive.

PURPOSE	TRANSACTION HASH	RECOVERED CHAIN
Exploit-contract deployment	`886027ee0876de8532d29e613eb901d653bfb2b5bd7f099d0dfc9c8163b24584`	Present
Initial native seed	`8aa902f02a6cfc4bf71544639ea08b1541d3250f158535dedce4075e62001103`	Present
NFT transfer to the contract	`e30c4c4513bb42ae82a1806677e7ba60789a56b81fee401a421de14dd6e6103f`	Present
Initial mixed-token seed	`510ef0ab618bc16a79eee6032fe0eb04632d0666948303e472d87bacfd7b0984`	Present
First exploit call	`95b2eb86622baa5503d5cf7cab38283185d5b011d516c66d54d9bc8c6a0affbf`	Excluded
Final exploit call	`793340cb04d0665bd9038bd07c9b2ffb3517f82991225e682cbb52d047d5def6`	Excluded
Final token recycling	`a7cd6a847a0a3489782bfff75012655692e3c147e1c704d60cc6e833380d90be`	Excluded

A.3 Verification performed for this report

On the live chain, through the public API at api.multiversx.com on 29 September 2026:

- Each published checkpoint header hash resolves to a block at round 33,384,826 (metachain nonce 33,336,396; Shard 0 nonce 33,359,761; Shard 1 nonce 33,349,726; Shard 2 nonce 33,354,137), epoch 2241, timestamp 06:37:45.000.
- The Shard 0 block at nonce 33,359,762, `340e851f…0ad7`, is at round 34,020,552 with the checkpoint block as its parent. The pre-recovery block at the same height, round 33,384,827, is not on the canonical chain, although the public API still listed it beside the canonical block on 29 September.
- The first exploit call, the final exploit call and the final token recycling return no result.
- The exploit contract holds 0.047609 EGLD, its seed balances of the seven bridged tokens and one unit of the NFT, and its code has not been upgraded. The operator account holds no unit of the NFT and sent nothing between its mixed-token seed at 06:35:39 (nonce 24) and a new transfer of its own funds on 27 September (nonce 25).
- Block timestamps match 0.6-second rounds counted from the published window boundaries, to the millisecond, from the contract deployment (round 33,384,529 at 06:34:46.8) to the present.
- One early request returned a cached, pre-recovery balance for the exploit contract. Repeated requests returned the live values above; anyone repeating these checks should do the same.

By computation, from the values in this report:

- All addresses carry valid bech32 checksums.
- MultiversX derives a contract address from its deployer's public key and account nonce. The operator's key at nonce 19 reproduces the exploit contract's address exactly, so the attribution of the deployment rests on arithmetic as well as on explorer data. Both keys map to Shard 0.
- The contract's pre-recovery balance equals its seed plus the 29 returned credits exactly: $0.047609 \times 2^{29} = 25{,}559{,}887.249408$ EGLD.
- Rounds 34,047,051 (21:00) and 34,158,051 (15:30) are 111,000 rounds and 18.5 hours apart, which fixes the round at 0.6 seconds, the block time introduced by Supernova.