Exploit of a Legacy Enjin NFT Contract on Ethereum

Date: 2026-08-27 | **Status:** Contained

Summary

On 25 August 2026, an exploit was observed on a legacy Ethereum ERC-1155 “CryptoItems” NFT contract, part of old infrastructure from before Enjin’s 2023 migration to Enjin Blockchain. The exploit has been **contained**.

- **Enjin Blockchain and native ENJ are not affected.**
- **The legacy ENJ ERC-20 token contract was not compromised.**
- The incident is limited to the legacy, non-canonical Ethereum CryptoItems NFT contract, superseded in December 2023.
- The affected NFT contract is now in a protective locked state, and no further assets can be drained.
- **No user action is required**, and your assets on Enjin Blockchain are safe.

What happened

`25 Aug, 18:42 UTC`	An exploit was observed against the legacy Ethereum CryptoItems contract, which holds Enjin’s early in-game NFT items. Using an authorization flaw, the attacker moved these items out of holders’ wallets without approval and melted them to redeem the ENJ backing in the contract’s reserve, the large majority of it from legacy proof-of-concept items.
`26 Aug, 00:02 UTC`	The contract was placed in a protective locked state, halting the operations the exploit relied on. The lock is a built-in safeguard included at deployment, a standard defensive measure.
`26 Aug (post-lock)`	Further attempts to continue the exploit were unsuccessful, and no further assets were drained.
`26 Aug (ongoing)`	The attacker converted the proceeds and transferred them off the Ethereum network. Enjin continues to monitor the funds and has shared indicators with exchanges and blockchain-analytics partners.

What this means for you

If you use Enjin Blockchain

Enjin Blockchain is a separate blockchain; both it and native ENJ are unaffected by this incident. Your NFTs on Enjin Blockchain are also unaffected: this vulnerability existed only in the specific legacy CryptoItems ERC-1155 contract on Ethereum, and does not apply generically to the ERC-1155 token standard or NFTs in general.

If you hold legacy ERC-20 ENJ on Ethereum

The legacy ENJ ERC-20 token contract was not compromised, and no wallet balances were moved. The ENJ that was drained was infused inside the CryptoItems gaming NFTs, and the loss was limited to the ENJ locked inside those specific gaming items.

If you held legacy CryptoItems NFTs on Ethereum

1. Were my legacy Ethereum items affected?
Only items still held on the old Ethereum CryptoItems contract were affected; anything migrated to Enjin Blockchain was never at risk. During the exploit, a number of these legacy items were transferred out of wallets and melted before the lock took effect. More than 80% of the legacy ERC-20 ENJ redeemed was backing for legacy proof-of-concept items, created during early development and of no ongoing significance. The rest, about 1.19 million ENJ, was backing for other legacy items, and only 415 wallets lost any ENJ at all. Among the wallets affected, 95% lost no ENJ, 97% lost under 1,000 ENJ, and 99.6% lost under 10,000 ENJ.

2. Do I need to do anything?
No. The legacy contract is locked and can no longer be used.

3. How do I access my legacy items now that the contract is locked?
Your canonical assets remain accessible on Enjin Blockchain. The legacy Ethereum items are frozen by the lock as a protective measure. Whether the contract can be safely upgraded and the lock lifted is under review. Removing the lock before the authorization flaw is fixed would expose legacy Enjin CryptoItems NFTs to the same risk. This is legacy, non-canonical infrastructure that was superseded in 2023.

4. Was my wallet or private key compromised?

No. This exploit was a flaw in the legacy contract's authorization logic, not a compromise of any wallet, private key, or seed phrase. You do not need to move funds, reset your wallet, or approve any transaction.

Ongoing response

- Investigating whether a safe upgrade and unlock of the legacy contract is feasible.
- Monitoring the attacker's on-chain activity and coordinating with exchanges and analytics providers.
- Providing updates as the situation develops.

> **Beware of scams.** Incidents like this attract phishing and impersonation. Enjin will never DM you first, ask for your seed phrase or private keys, or request wallet approvals to "recover" assets.

Affected contract (Ethereum mainnet): `0xfaaFDc07907ff5120a76b34b731b278c38d6043C`