Shut down of 0x Exchange v2.0 contract and migration to patched version

Will Warren
Jul 13, 2019 · 3 min read

📌 **Final Update (07/13):** We have patched and re-deployed the entire 0x smart contract pipeline from scratch, updated our developer tools and packages, 0x Instant, and 0x Launch Kit. As previously mentioned, we have confirmed that the vulnerability found in the 0x v2.0 Exchange contract was not exploited and no user funds have been lost. Please expect a formal post-mortem blog post in the next couple of days.

We sincerely thank all of the teams in the ecosystem for their understanding, patience, and cooperation throughout this process. For any teams still requiring assistance in migrating to the newly deployed contracts, please reach out to any member of the 0x Core Team on our Discord server.

📌 **Update (07/12 — 11:51 PM PT):** Please find the patched contract addresses below. Developer tools and packages will be updated to reflect these changes tomorrow morning.

ERC20Proxy: 0x95e6f48254609a6ee006f7d493c8e5fb97094cef
ERC721Proxy: 0xefc70a1b18c432bdc64b596838b4d138f6bc6cad
MAP: 0xef701d5389ae74503d633396c4d654eabedc9d78
Exchange: 0x080bf510fcbf18b91105470639e9561022937712
APOwner: 0xdffe798c7172dd6deb32baee68af322e8f495ce0
Forwarder: 0x76481caa104b5f6bccb540dae4cefaf1c398ebea
OrderValidator: 0xa09329c6003c9a5402102e226417738ee22cf1f2

📌 **Update (07/12 — 09:43 PM PT):** After analyzing historical trade logs, we have confirmed that the vulnerability found in the 0x v2.0 Exchange contract was not exploited and no user funds have been lost.

. . .

Today (7/12), at approximately 4:30 PM PT, we were made aware of a potential exploit in the 0x v2.0 Exchange contract by a third-party security researcher samczsun. This vulnerability would allow an attacker to fill certain orders with invalid signatures. **This vulnerability does not affect the ZRX token contract; your digital assets are safe**.

After verifying the vulnerability internally at 0x and out of an abundance of caution, we have used the AssetProxyOwner contract to shut down the v2.0 Exchange and all AssetProxy contracts to prevent this vulnerability from being exploited. The contracts were shut down at approximately 7:45 PM PT. To the best of our knowledge, no one has exploited this vulnerability and no user funds have been lost**.** Unfortunately, this also means the currently deployed 0x contracts cannot process trades and are unable to be used.

A patched version of the Exchange contract — that we are confident fixes this vulnerability — and new AssetProxy contracts are being deployed to the Ethereum mainnet and we expect them to be ready to use later tonight.

Exploit Description

We are doing our best to verify that other smart contracts are not vulnerable to this exploit before disclosing it publicly in a formal post-mortem.

📌 **Update (07/13–10:30 PM PT):**

- @samczsun has provided a detailed explanation of the vulnerability here.

Immediate Next Steps

Teams will need to point to the patched and newly deployed Exchange and AssetProxy contracts as well as clear their orderbooks of outstanding orders. Users will need to reset their allowances for the new 0x AssetProxy contracts. This post will be updated with the new addresses post-deployment.

On behalf of the 0x core team, I sincerely apologize. Since the beginning, we've set an extremely high bar for code quality, test hygiene, and all independent security auditors that we work with. We understand the existence of a potentially critical bug deserves

serious reflection. We hope to discuss this issue with the broader community in the next few days to ensure all smart contract security practices for 0x protocol are transparent, rigorous, and community-vetted.

We also want to extend our sincerest gratitude to samczsun. We continue to offer a generous bug bounty to white hat hackers and community members that identify potential vulnerabilities.

If you have any subsequent questions or just want to speak with someone from the Core Team, please do not hesitate to reach out on Discord. We will spend as much time as necessary to work through any technical issues.

Ethereum 0x Protocol