Proskauer

Smart Contract Bug Leads Exchanges to Halt ERC-20 Token Trading

Blockchain and the Law Blog on **April 27, 2018**

When a smart contract coding vulnerability resulted in the Parity wallet "freeze" that compromised over $150 million worth of user funds, we discussed the pitfalls of unsecure code in the context of cryptoassets and the extent to which software developers might be held liable to their users for losses arising from mistakes in, or the exploitation of, the open source software they release into the world.

On Thursday, yet another possible coding vulnerability emerged – this time with the protocol underlying certain tokens themselves – as various exchanges suspended trading in ERC-20 tokens due to a discovery by security researchers of a smart contract bug known as batchOverflow.

According to researchers, attackers taking advantage of batchOverflow could generate a large amount of tokens from a vulnerable ERC-20 contract, then seek to deposit those tokens into a normal Ethereum address.

Such an attack raises issues of potential theft, unjust enrichment, fraud and market manipulation for the attackers. Furthermore, there is the question of whether liability could attach to developers who overlooked the batchOverflow bug in the first place (notably, the vulnerable function is not part of the official ERC-20 standard and was only implemented for a limited number of tokens).

As affected cryptoasset organizations, customers and exchanges continue to investigate, it remains to be seen whether and how any unauthorized transactions will be remedied. The questions abound:

Will victims and community members advocate for a remedial fork? (Parity, for their part, has recently pronounced that they have no intention to utilize a fork to rescue their wallets' frozen funds.)

How will industry standards in the U.S. and other jurisdictions evolve to reflect the role of secure software in the “Internet of Value”?

Finally, will legal institutions be mobilized?

View Original