OpenZeppelin Uncovers Vulnerability in Libra's Move IR Compiler

OPENZEPPELIN SECURITY | SEPTEMBER 9, 2019

Security Audits

SAN FRANCISCO, September 10, 2019 – OpenZeppelin, a leader in blockchain infrastructure security, today announced that its research team discovered a vulnerability in Libra's Move IR compiler. The company found a problem in Libra's intermediate representation language compiler, the Move IR, that could allow cybercriminals to exploit the yet-to-be-launched cryptocurrency network. After being alerted, the Libra team applied a patch to avert an issue that could have affected millions of Libra users once the network is launched.

The newly discovered vulnerability could allow malicious actors to publish deceitful Move modules that would look one way to a user but behave in a different manner. For example, a digital wallet could look like it has frozen new deposits and would release them after a prescribed length of time. But those funds would never be released or worse, would be diverted.

According to OpenZeppelin's research team, the vulnerability could let malicious actors write inline comments that could act like executable code. This issue would render the Move IR module source files with inline comments untrustworthy— a liability in a blockchain setting where auditability substitutes for trust.

"As cryptocurrency continues to grow in popularity, it is vital for companies to audit and ensure that their networks are secure," said Demian Brener, OpenZeppelin CEO. "Libra is groundbreaking, and

illustrated why they needed to address this issue quickly.”

OpenZeppelin alerted the Libra Association to the issue. The organization addressed the vulnerability and released a patch. For a more detailed look at what the OpenZeppelin found, read their technical description in the OpenZeppelin blog.

About OpenZeppelin

OpenZeppelin builds developer tools and performs security audits for decentralized systems that power multimillion-dollar economies. The leader in blockchain infrastructure security, OpenZeppelin has set industry standards for building secure, decentralized systems and has gained the trust from industry leaders including Brave, Coinbase, Ethereum Foundation, Compound and Augur. OpenZeppelin built and maintains the world’s leading Open Source library for smart contract development with more than one million downloads and 180 contributors. Follow OpenZeppelin on Twitter and our blog.

Related Posts

Beefy Zap Audit

BeefyZapRouter serves as a versatile intermediary designed to execute users' orders through routes...

OpenBrush Contracts Library Security Review

OpenBrush is an open-source smart contract library written in the Rust

Linea Bridge Audit

Linea is a ZK-rollup deployed on top of Ethereum. It is designed to be EVM-compatible and aims to...

OpenZeppelin

Defender Platform

Secure Code & Audit
Secure Deploy
Threat Monitoring
Incident Response
Operation and Automation

Services

Smart Contract Security Audit
Incident Response
Zero Knowledge Proof Practice

Learn

Docs
Ethernaut CTF
Blog

Company

About us
Jobs
Blog

Contracts Library

Docs

Privacy | Terms of Use