

黑客从Poolz Finance窃取了3.9亿美元，这是继1.8亿美元的Euler Finance漏洞之后的又一次安全事件。

- 由于一个漏洞，Poolz Finance在Binance智能链和Polygon区块链上损失了390,000美元
- Poolz是一个跨链去中心化的IDO平台，专注于Web3的开发。
- MetatrusterLabs分析发现，一个算术溢出问题导致了该漏洞。

MetatrusterLabs周三发现，在Binance智能链和Polygon上，一次黑客攻击使Poolz Finance损失了约39万美元。

这家区块链安全公司指出，黑客可能是由于算术溢出问题而发生的。

关于Poolz Finance黑客，我们应该知道什么

MetatrusterLabs分析表明，Poolz Finance存在算术溢出问题。在计算机科学中，这是一个较大的操作产量对相对较小的存储系统的问题。同时，MetatrusterLabs发现同一发件人在代币归属合约上的重复模式。

**Hudson Jameson** @hudsonjameson · Follow

\$20m and no hunt vs \$200m and you're chased heavily by on-chain sleuths wanting \$1m reward...

This seems like a no brainer.

**0xngmi (llamazip arc)** @0xngmi  
euler just sent an on-chain message to the hacker

`0x00 (Euler Deployer)`  
`0xbb66ce9666706962c277e3e81a3ba8720bfb995cb (Euler Finance Exploiter 2)`

0 ETH (\$0.00)  
0.0008792721192088 ETH (\$1.50)  
36.21384345 Gwei (0.00000003621384346 ETH)

24,260 / 24,200 (100%)  
Base: 36.125567019 Gwei | Max: 36.21384346 Gwei | Max Priority: 36.21384346 Gwei

Value: 0.0008792721192088 ETH (\$1.50) | Fee: 0 ETH (\$0.00)

Gas Used: 2,039,188 | Gas Price: 142 | Possible to Revert: 164

Following up on our message from yesterday. If 90% of the funds are not returned within 24 hours, tomorrow we will launch a \$1M reward for information that leads to your arrest and the return of all funds.

View on Etherscan

8:00 AM · Mar 15, 2023

74 ❤️ Reply Copy link

据报道，黑客已将该协议中的资金转移到两个新账户。这些钱包里装了大量的DAI稳定币和以太坊（ETH）。

DeFi协议仍然是攻击目标

今年2月，Platypus在一次闪电贷攻击中损失了850万美元以上。根据Chainalysis的报告显示，2022年全球安全事件中受害者失去了价值38亿美元的加密货币，成为史上最大的黑客事件年份。其中大部分来自DeFi协议。

区块链安全公司Halborn的首席运营官David Schwed表示，这些攻击基于Web2攻击模式。他在与Chainalysis的对话中说：“我们看到的许多黑客攻击不一定是针对web3的密钥泄露攻击。它们是具有web3含义的传统Web2攻击”。

下面是MetatrustLabs对此次安全事件的分析详情：

## Poolz Finance漏洞

### 摘要

攻击者(0x190cd)通过算术溢出欺骗了他实际存入的合约(0x058ba)。该合约的版本低于0.8.0，缺乏算术溢出检查。

### 攻击者

<https://bscscan.com/address/0x190cd736f5825ff0ae0141b5c9cb7fcd042cef2a>

### 攻击的合约

<https://bscscan.com/address/0x058bae36467a9fc5e1045dbdffc2fd65b91c2203>

<https://etherscan.io/address/0x058bae36467a9fc5e1045dbdffc2fd65b91c2203>

### 被攻击的合约

<https://bscscan.com/address/0x8bfaa473a899439d8e07bf86a8c6ce5de42fe54b>

<https://etherscan.io/address/0x2cc4a6c6d5ff183d7e3c7e33e9bc10d55bdba8ea8>

### 交易

<https://bscscan.com/tx/0x39718b03ae346dfe0210b1057cf9f0c378d9ab943512264f06249ae14030c5d5>

<https://bscscan.com/tx/0xab09638803c66d802fc83e088da6fa894a714ae2d4df707c6f4bb1b42594f5ac>

<https://bscscan.com/tx/0x24cb4df2bd6829c0736750aa51ee9c03982cf70b9cd30f8b8259395f1ba10030>

<https://etherscan.io/tx/0x118a617bddd1c14810113be81ce336f28cc1ee7a7b538a07184b93e7c51bdc00>

### 操作步骤

- 攻击者通过算术溢出伪造其实际存入的合约。
- 攻击者从合约中提取代币。

### 根本原因

实际转移的金额是1，但攻击的记录金额是115792089237316195423570985008687907853269984665640502182660492372007802789937和61856797091635905326850000。