12月13日，根据区块链安全审计公司Beosin的BeoSin鹰眼安全风险监控、预警与阻断平台监测，ElasticSwap遭到攻击。由于契约中添加流动性和去除流动性的计算方法不一致，所以在添加流动性的函数中使用了常规的常数K值算法，而在去除流动性的函数中，直接接收当前池中两个代币的余额进行计算，攻击者先添加流动性。之后，一定量的USDC。e将被转移到TIC-USDC交易池。这时，USDC号。应该转给攻击者的e已经乘以LP代币数，也就是几倍，然后攻击者会调用流动性移除方法获利22,454AVAX。同时以太坊链上ElasticSwap下的AMPL-USDC池也遭到了同样的攻击，攻击者获利约445ETH。到目前为止，这两笔有利可图的资金已经存入了攻击者&#039；的账户。

第一次攻击tx；

第一个攻击者账号：0x25FDE76a52d01c83e31D2D5E1d2011ff103c56。

第二次攻击tx；

thesecondattackeraccount:0xbedbed6a353c9caa4894a7a7E5F883e32967.