



bitshares

HacktheDex

## Report 20181206A

### Type

Blockchain halt provocation

### Description

Currently it is possible for an asset to be borrowed into supply, even if it would exceed the GRAPHENE\_MAX\_SHARE\_SUPPLY. If a global settlement would happen, the chain would halt as a result of overflow multiplication on any supply greater than GRAPHENE\_MAX\_SHARE\_SUPPLY.

### Review

OWASP Rating	
Likelihood	Medium
Impact	High
Severity	High

Possible attack vector: Broadcast a transaction that causes a blockchain halt.

Reviewers: Ryan Fox, Peter Conrad, John Jones

### Resolution

BitShares core [was fixed publicly](#) preceded by a mandatory upgrade for block producers on 7th of December.

### Reward Consensus

Reward	15,000 bitUSD
--------	---------------