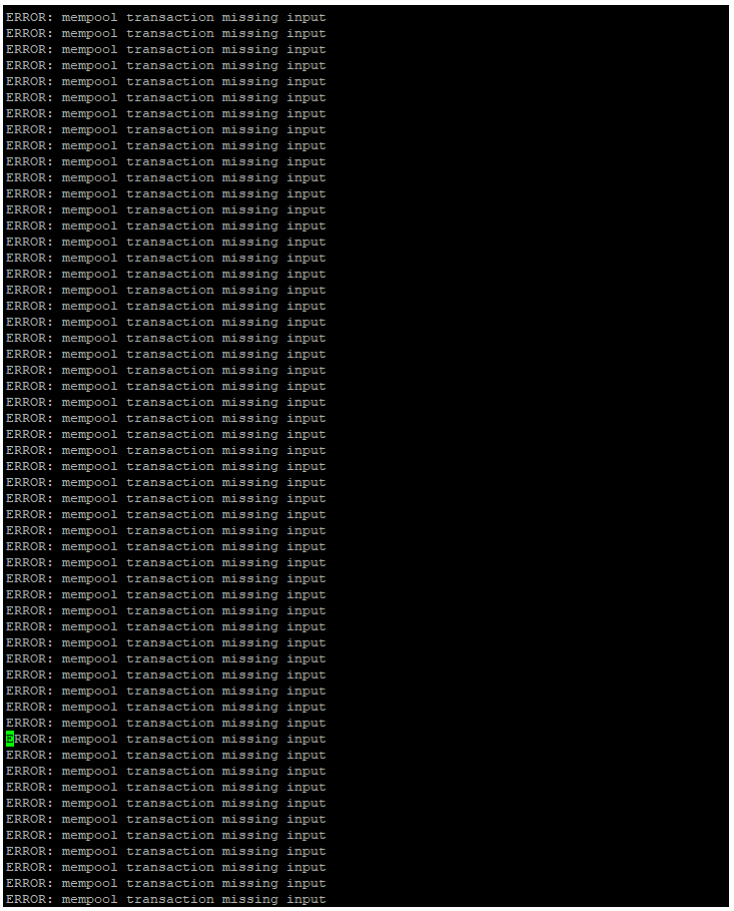
Blockchain Situation:

The bitFlowers chain was attacked leading up to the network disruption on the 28th of May 2021. The team acted quickly, and all exchange wallets were put into maintenance mode, all seed nodes were stopped, and chain movement was halted. This was necessary in order to locate the issue and figure out a solution.

Chain Analysis:

As soon as the chain was stopped, the team made a deep investigation of the debug file of the seed nodes to find the problem.



The debug file was flooded with messages about block errors. As a result, numerous wallets were forked and running on their own chain causing balance errors.

Solution:

After a thorough review, a known bug in the Scrypt code called "*FutureDrift bug*" was discovered.

The *FutureDrift* code is responsible for checking the timestamps of blocks in the chain in relation to the mempool and determine if the block is orphaned or not. This bug was exploited when the wallet was in the POS phase.

When checking the code, we could see that the original code had the following parameters:

-Past Check: Time actual -300 secs

-Future Check: Time actual +300 secs

To correct this the new code has been updated to:

-Time actual +15 secs

With this code update, the block timestamps are more adjusted and prevent numerous forks. A protocol increase was also included thereby forcing a wallet upgrade to be on the same version. And finally, checkpoints were added to further ensure chain stability.

Protocol update:

6 src/version.h

```
@@ -30,21 +30,21 @@ static const int DATABASE_VERSION = 70509;
 // network protocol versioning
 //

-static const int PROTOCOL_VERSION = 2000000;
+static const int PROTOCOL_VERSION = 3000000;

 // intial proto version, to be increased after version/verack negotiation
 static const int INIT_PROTO_VERSION = 209;

 // disconnect from peers older than this proto version
-static const int MIN_PEER_PROTO_VERSION = 1009999;
+static const int MIN_PEER_PROTO_VERSION = 3000000;

 // nTime field added to CAddress, starting with this version;
 // if possible, avoid requesting addresses nodes older than this
 static const int CADDR_TIME_VERSION = 31402;

 // only request blocks from nodes outside this range of versions
 static const int NOBLKS_VERSION_START = 1;
-static const int NOBLKS_VERSION_END = 1009999;
+static const int NOBLKS_VERSION_END = 2009999;

 // BIP 0031, pong message, is enabled for all versions AFTER this one
 static const int BIP0031_VERSION = 60000;
```

Checkpoints:

5 src/checkpoints.cpp

```
@@ -32,6 +32,11 @@ namespace Checkpoints
         (  100000, uint256("0x7b8d36e724d673665ac780fbb35fc6b9c93aa26c5e88e21c9b34ca41435876b4") )
         (  200000, uint256("0x000000000160400d58cdc1131e7bd49f611b5bd2a223f6ee0481a8da1946c44") )
         (  300000, uint256("0x0000000000136f98c101dcadd5c3b0cc47ce42bdaeba3718d5f04a95f0660642") )
+        (  320000, uint256("0xa05304e0080afb3b6f9b5c3261c9dba4f40c4522bfd81a3c4fa14c5125e652b2") )
+        (  350000, uint256("0x815d972777a0d97171edd64b109f6017021655651748943c98cfab7c4fbeadf2") )
+        (  390000, uint256("0x4942f05b8f8c96685f8a7b467902ecd28087eb051b8d12cd14ee7ef01b54ee42") )
+        (  410000, uint256("0xb6748e1a4e412fa6ff8a33e491b0b24b0c4caf4ae5ac4019acfabbcb39e9e51e") )
+        (  415000, uint256("0xbf59571fd59a04913987176426a0ac61cc7d378667995b129e45e95b296cec4e") )
         ;

     // TestNet has no checkpoints
```

Future Improvements:

This exploit was discovered and corrected quickly. Development has resumed on bitFlowers with an increase in the security of the seed servers, rigorous checks on block stake generation, and additional resources to eliminate future attacks.