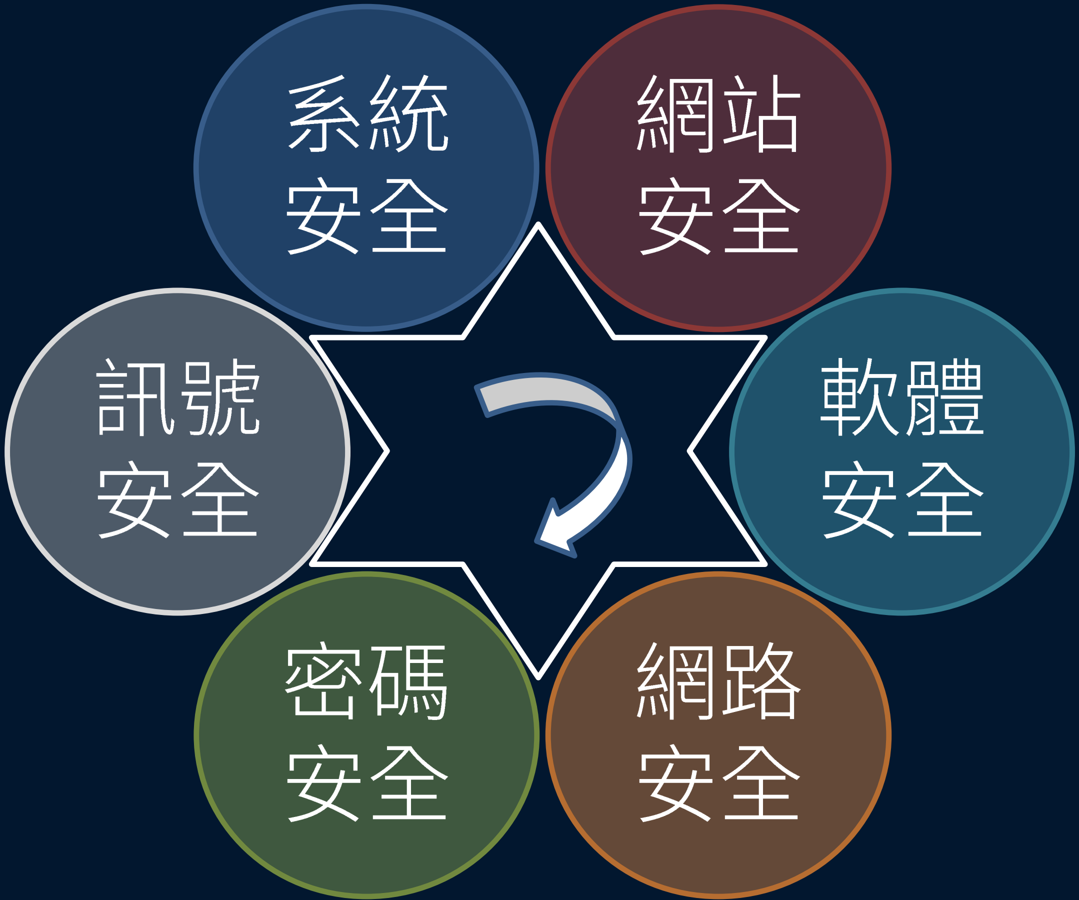
攻擊者視角

Funny Systems

Kuon

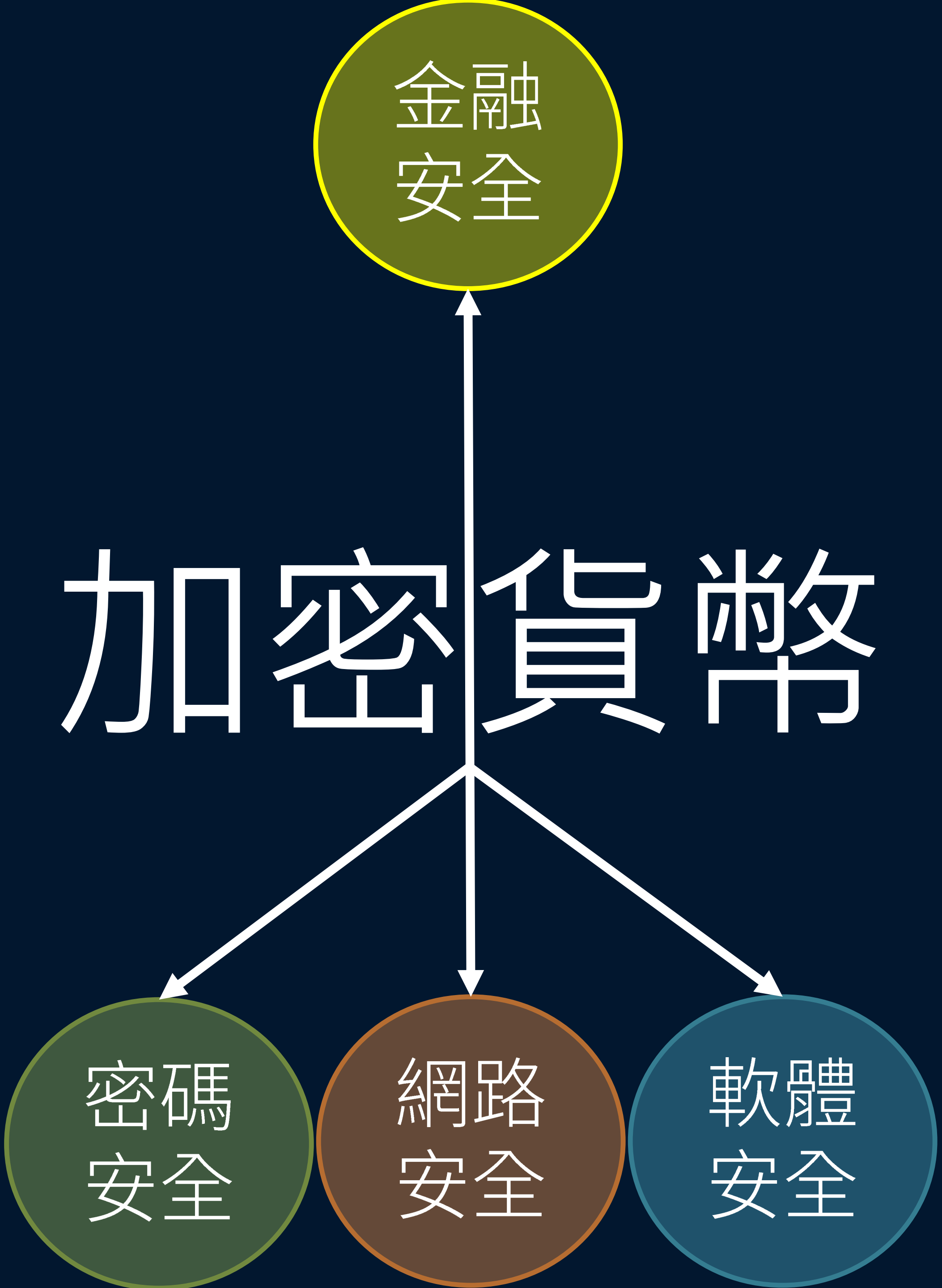
喜歡學習，特別是「安全技術」。



相信

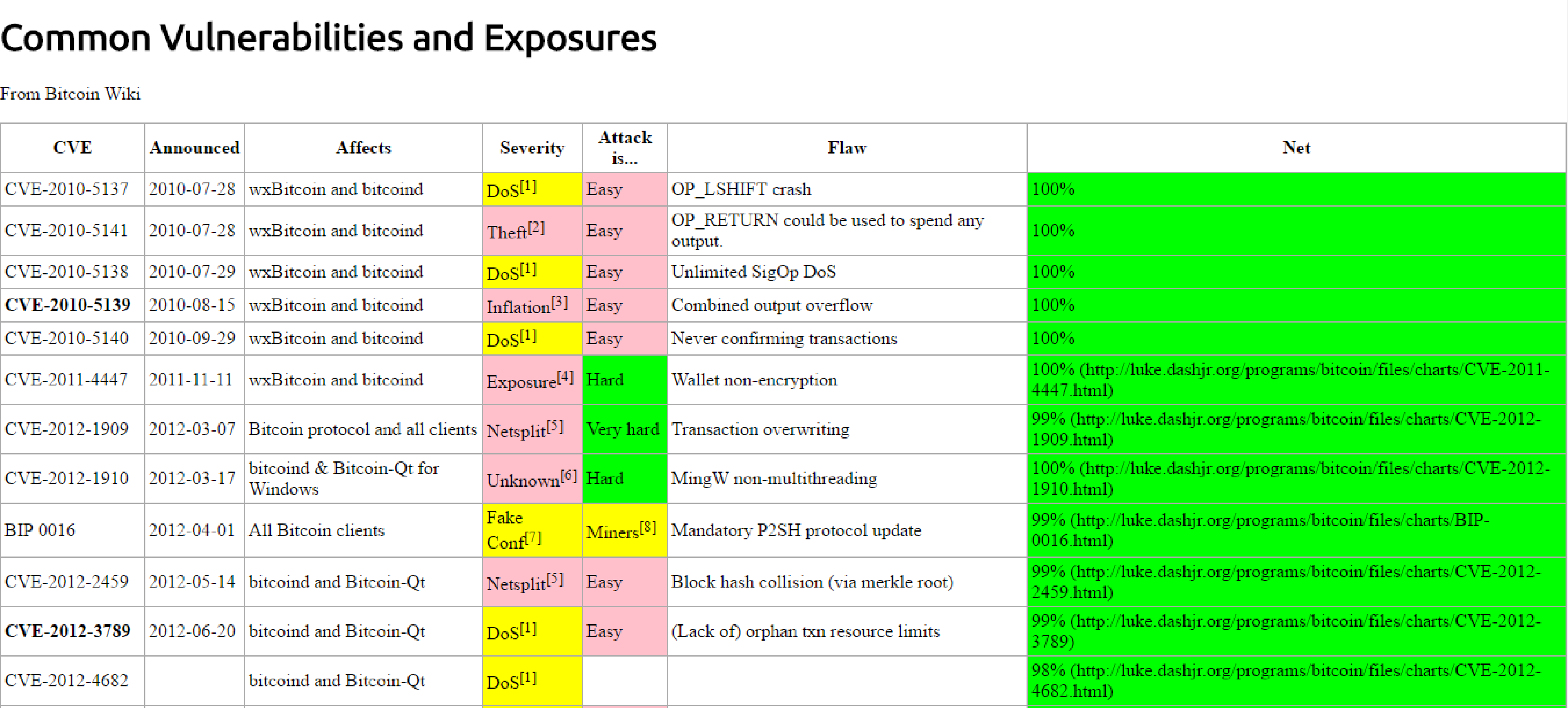
加密貨幣

?


金融
安全
加密貨幣
密碼
安全
網路
安全
軟體
安全

CVE

軟體
安全



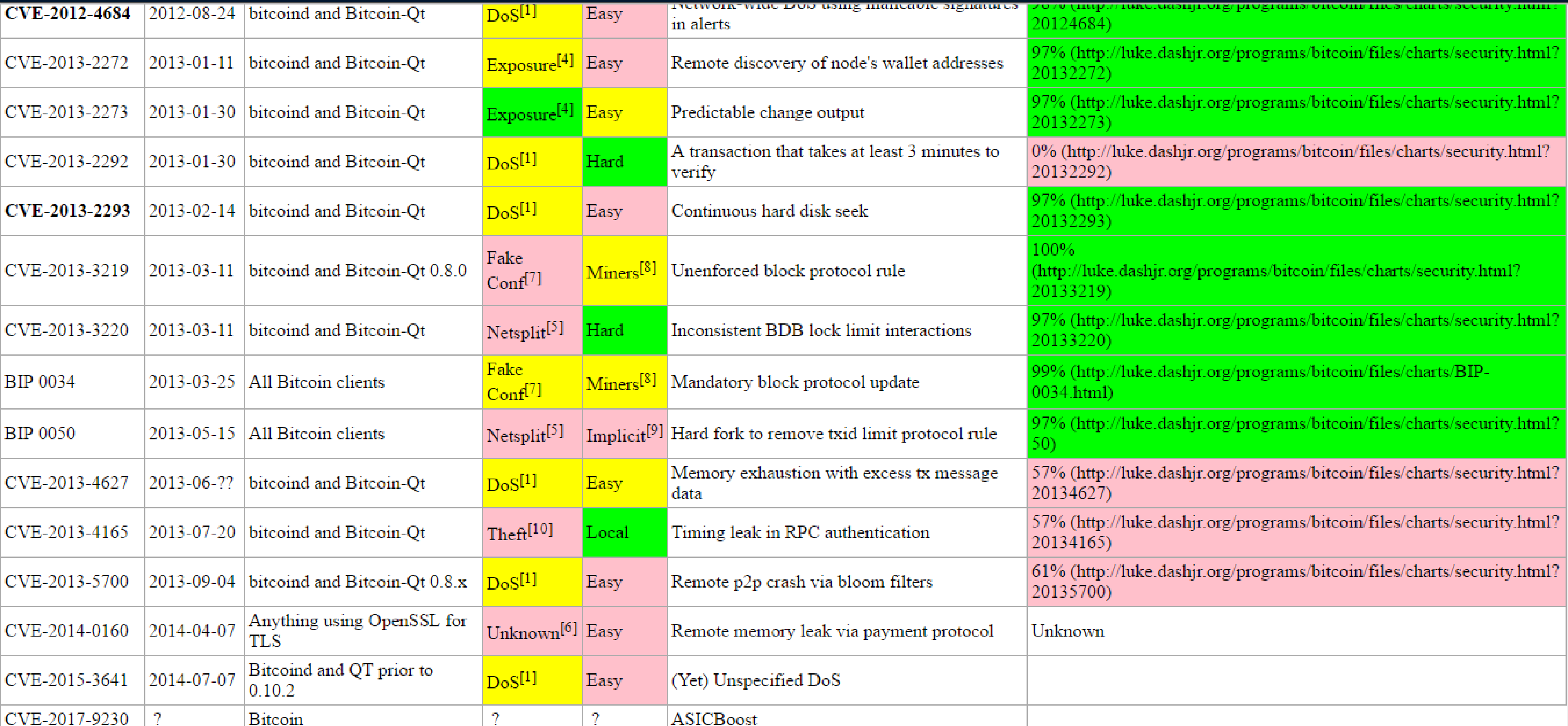
Common Vulnerabilities and Exposures

From Bitcoin Wiki

CVE	Announced	Affects	Severity	Attack is...	Flaw	Net
CVE-2010-5137	2010-07-28	wxBitcoin and bitcoind	DoS[1]	Easy	OP_LSHIFT crash	100%
CVE-2010-5141	2010-07-28	wxBitcoin and bitcoind	Theft[2]	Easy	OP_RETURN could be used to spend any output.	100%
CVE-2010-5138	2010-07-29	wxBitcoin and bitcoind	DoS[1]	Easy	Unlimited SigOp DoS	100%
CVE-2010-5139	2010-08-15	wxBitcoin and bitcoind	Inflation[3]	Easy	Combined output overflow	100%
CVE-2010-5140	2010-09-29	wxBitcoin and bitcoind	DoS[1]	Easy	Never confirming transactions	100%
CVE-2011-4447	2011-11-11	wxBitcoin and bitcoind	Exposure[4]	Hard	Wallet non-encryption	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2011-4447.html)
CVE-2012-1909	2012-03-07	Bitcoin protocol and all clients	Netsplit[5]	Very hard	Transaction overwriting	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-1909.html)
CVE-2012-1910	2012-03-17	bitcoind & Bitcoin-Qt for Windows	Unknown[6]	Hard	MingW non-multithreading	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-1910.html)
BIP 0016	2012-04-01	All Bitcoin clients	Fake Conf[7]	Miners[8]	Mandatory P2SH protocol update	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/BIP-0016.html)
CVE-2012-2459	2012-05-14	bitcoind and Bitcoin-Qt	Netsplit[5]	Easy	Block hash collision (via merkle root)	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-2459.html)
CVE-2012-3789	2012-06-20	bitcoind and Bitcoin-Qt	DoS[1]	Easy	(Lack of) orphan txn resource limits	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-3789)
CVE-2012-4682		bitcoind and Bitcoin-Qt	DoS[1]			98% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-4682.html)

CVE

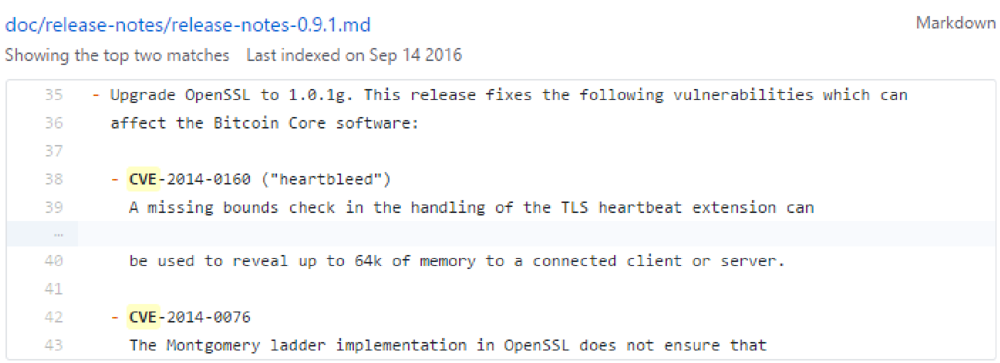
軟體
安全



CVE-2012-4684	2012-08-24	bitcoind and Bitcoin-Qt	DoS[1]	Easy	Network-wide DoS using malleable signatures in alerts	98% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20124684)
CVE-2013-2272	2013-01-11	bitcoind and Bitcoin-Qt	Exposure[4]	Easy	Remote discovery of node's wallet addresses	97% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132272)
CVE-2013-2273	2013-01-30	bitcoind and Bitcoin-Qt	Exposure[4]	Easy	Predictable change output	97% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132273)
CVE-2013-2292	2013-01-30	bitcoind and Bitcoin-Qt	DoS[1]	Hard	A transaction that takes at least 3 minutes to verify	0% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132292)
CVE-2013-2293	2013-02-14	bitcoind and Bitcoin-Qt	DoS[1]	Easy	Continuous hard disk seek	97% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132293)
CVE-2013-3219	2013-03-11	bitcoind and Bitcoin-Qt 0.8.0	Fake Conf[7]	Miners[8]	Unenforced block protocol rule	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20133219)
CVE-2013-3220	2013-03-11	bitcoind and Bitcoin-Qt	Netsplit[5]	Hard	Inconsistent BDB lock limit interactions	97% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20133220)
BIP 0034	2013-03-25	All Bitcoin clients	Fake Conf[7]	Miners[8]	Mandatory block protocol update	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/BIP-0034.html)
BIP 0050	2013-05-15	All Bitcoin clients	Netsplit[5]	Implicit[9]	Hard fork to remove txid limit protocol rule	97% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?50)
CVE-2013-4627	2013-06-??	bitcoind and Bitcoin-Qt	DoS[1]	Easy	Memory exhaustion with excess tx message data	57% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20134627)
CVE-2013-4165	2013-07-20	bitcoind and Bitcoin-Qt	Theft[10]	Local	Timing leak in RPC authentication	57% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20134165)
CVE-2013-5700	2013-09-04	bitcoind and Bitcoin-Qt 0.8.x	DoS[1]	Easy	Remote p2p crash via bloom filters	61% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20135700)
CVE-2014-0160	2014-04-07	Anything using OpenSSL for TLS	Unknown[6]	Easy	Remote memory leak via payment protocol	Unknown
CVE-2015-3641	2014-07-07	Bitcoind and QT prior to 0.10.2	DoS[1]	Easy	(Yet) Unspecified DoS	
CVE-2017-9230	?	Bitcoin	?	?	ASICBoost	

CVE-2014-0160

軟體安全



doc/release-notes/release-notes-0.9.1.md

Markdown

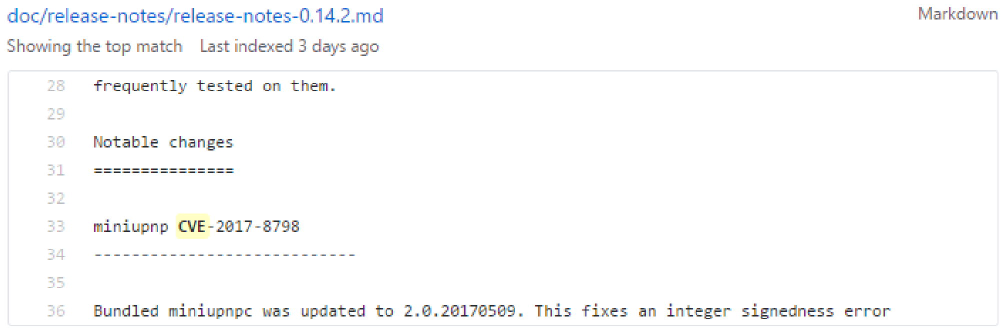
Showing the top two matches Last indexed on Sep 14 2016

```
- Upgrade OpenSSL to 1.0.1g. This release fixes the following vulnerabilities which can
  affect the Bitcoin Core software:

  - CVE-2014-0160 ("heartbleed")
    A missing bounds check in the handling of the TLS heartbeat extension can
…
    be used to reveal up to 64k of memory to a connected client or server.

  - CVE-2014-0076
    The Montgomery ladder implementation in OpenSSL does not ensure that
```

密碼安全

CVE-2017-8198

軟體
安全



doc/release-notes/release-notes-0.14.2.md

Markdown

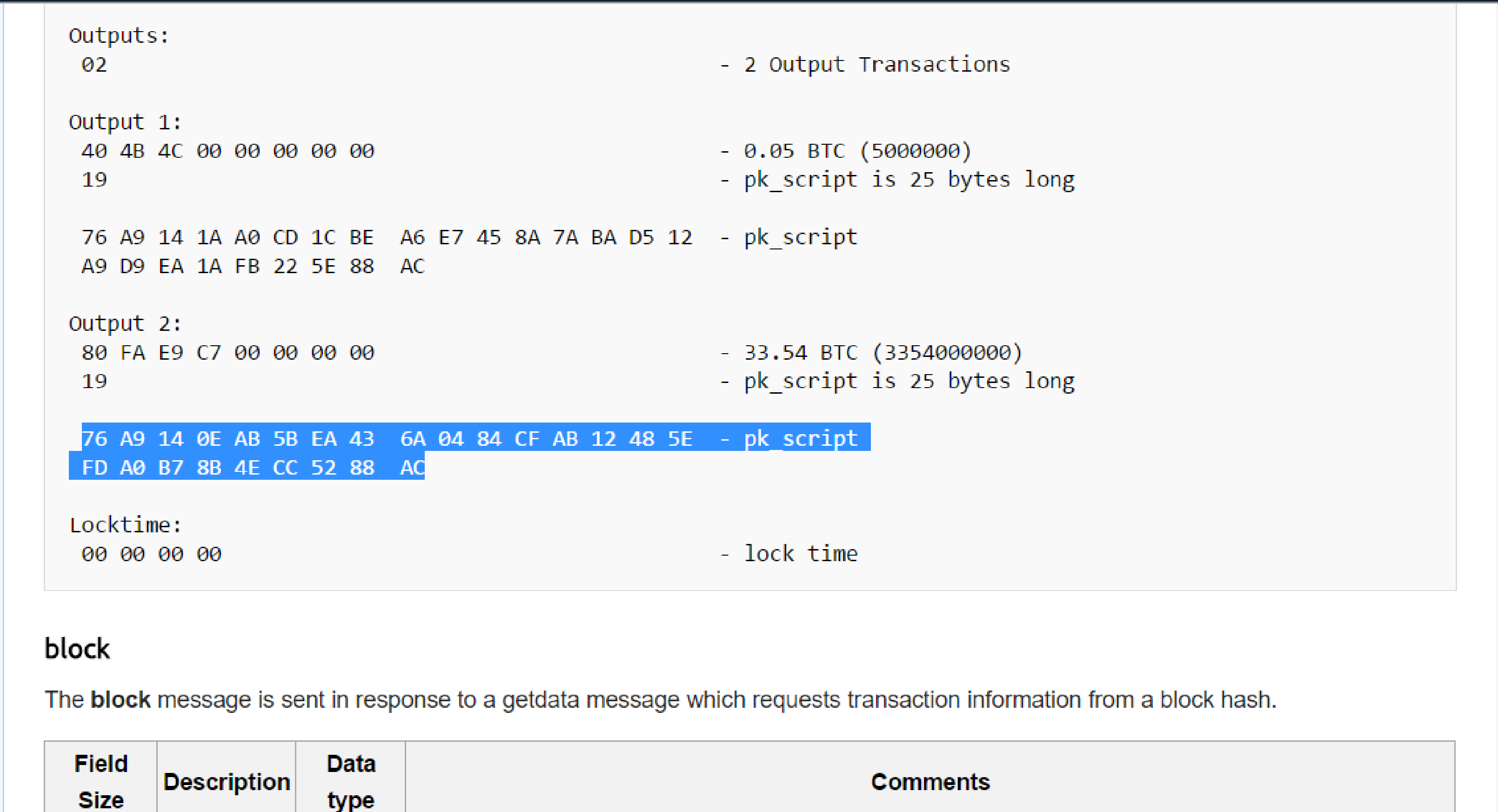
Showing the top match Last indexed 3 days ago

```
frequently tested on them.

Notable changes
===============

miniupnp CVE-2017-8798
----------------------------

Bundled miniupnpc was updated to 2.0.20170509. This fixes an integer signedness error
```

網路
安全

Protocol - Transaction

網路
安全



```
Outputs:
 02                                                - 2 Output Transactions

Output 1:
 40 4B 4C 00 00 00 00 00                           - 0.05 BTC (5000000)
 19                                                - pk_script is 25 bytes long

 76 A9 14 1A A0 CD 1C BE  A6 E7 45 8A 7A BA D5 12  - pk_script
 A9 D9 EA 1A FB 22 5E 88  AC

Output 2:
 80 FA E9 C7 00 00 00 00                           - 33.54 BTC (3354000000)
 19                                                - pk_script is 25 bytes long

 76 A9 14 0E AB 5B EA 43  6A 04 84 CF AB 12 48 5E  - pk_script
 FD A0 B7 8B 4E CC 52 88  AC

Locktime:
 00 00 00 00                                       - lock time
```

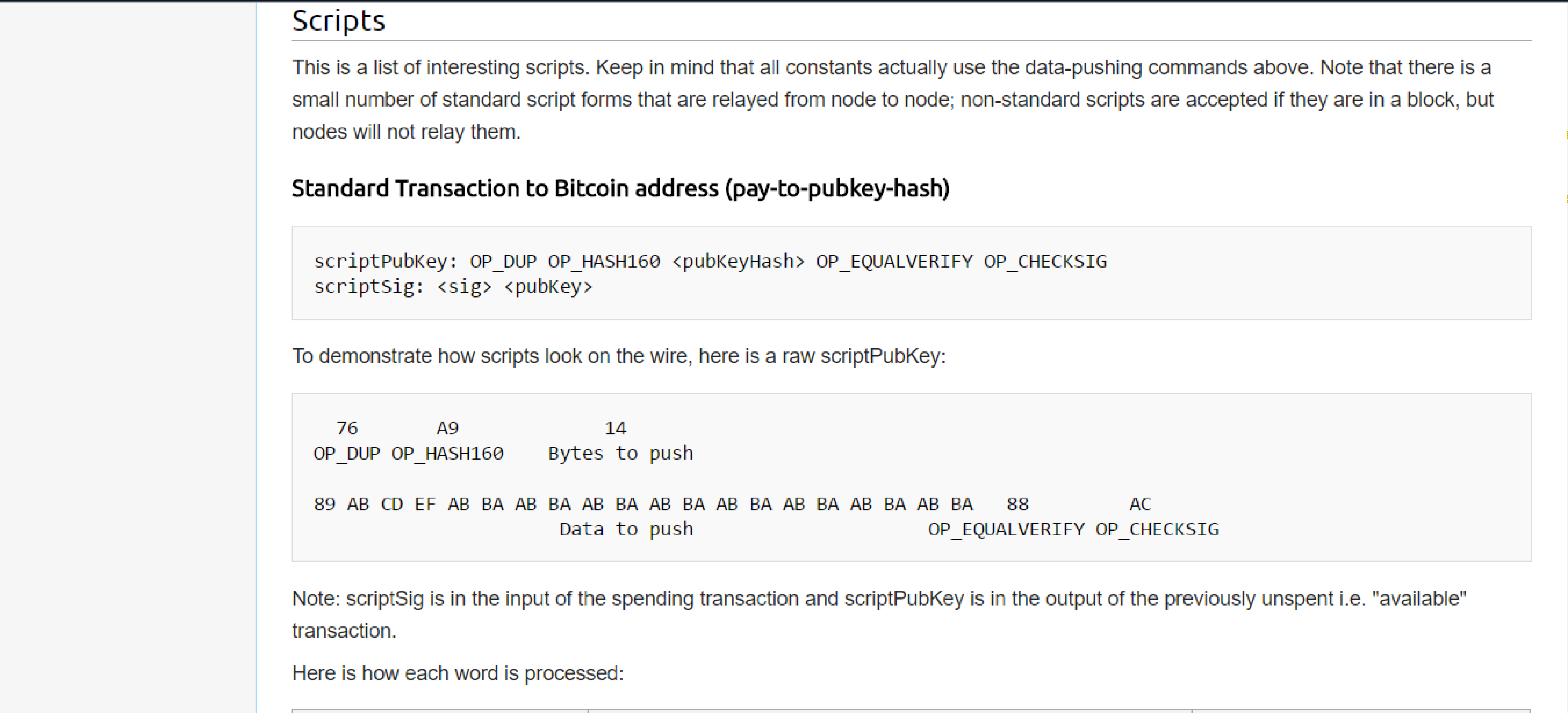
block

The **block** message is sent in response to a getdata message which requests transaction information from a block hash.

Field Size	Description	Data type	Comments

Script - Bytecode

金融
安全



Scripts

This is a list of interesting scripts. Keep in mind that all constants actually use the data-pushing commands above. Note that there is a small number of standard script forms that are relayed from node to node; non-standard scripts are accepted if they are in a block, but nodes will not relay them.

Standard Transaction to Bitcoin address (pay-to-pubkey-hash)

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
scriptSig: <sig> <pubKey>
```

To demonstrate how scripts look on the wire, here is a raw scriptPubKey:

```
  76       A9             14
OP_DUP OP_HASH160    Bytes to push

89 AB CD EF AB BA AB BA AB BA AB BA AB BA AB BA AB BA AB BA   88         AC
                      Data to push                     OP_EQUALVERIFY OP_CHECKSIG
```

Note: scriptSig is in the input of the spending transaction and scriptPubKey is in the output of the previously unspent i.e. "available" transaction.

Here is how each word is processed:

惡意

vs.

完整性

不可否認性

匿名識別度

可追蹤性

相信

匿名數位貨幣

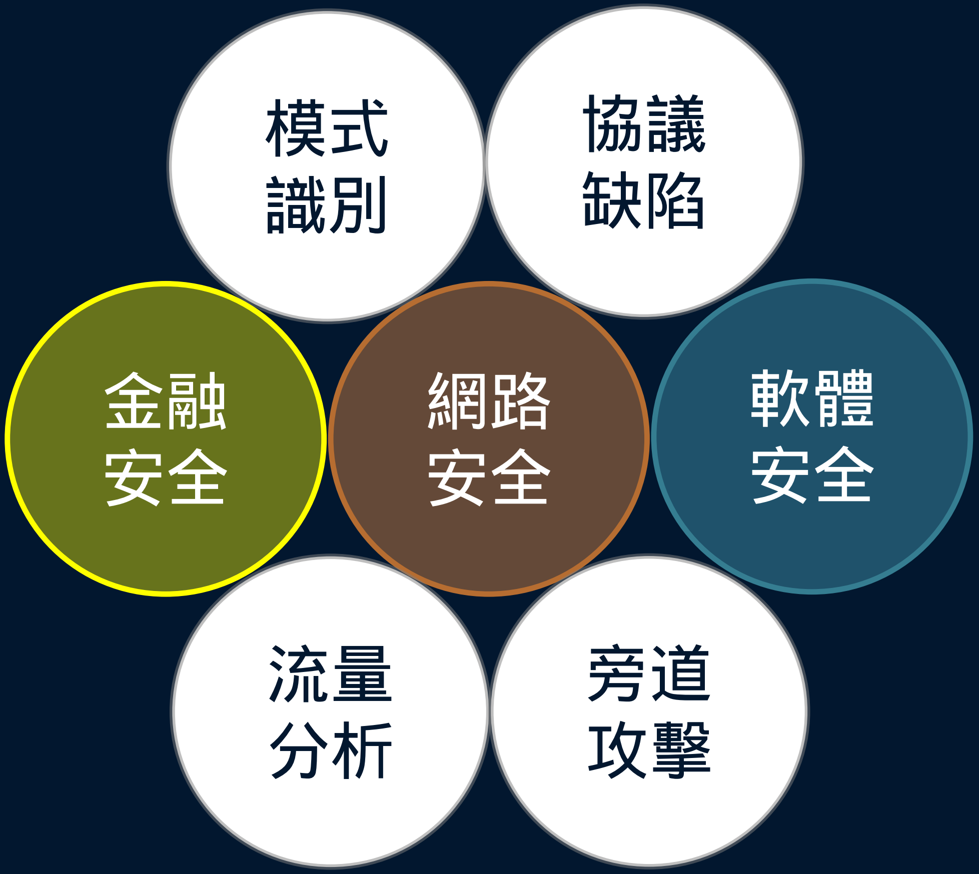
?

三大挑戰

1. 金融監理 » 非典型交易模式
2. Pseudonymous » 多(匿名)帳戶
3. 科技偵查 » (跨國) VPN & Tor

交易-帳號-實名

領域知識



模式識別

協議缺陷

金融安全

網路安全

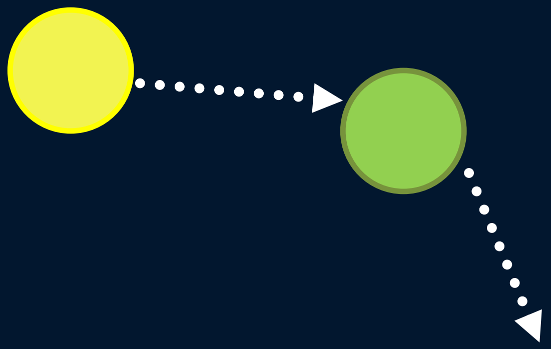
軟體安全

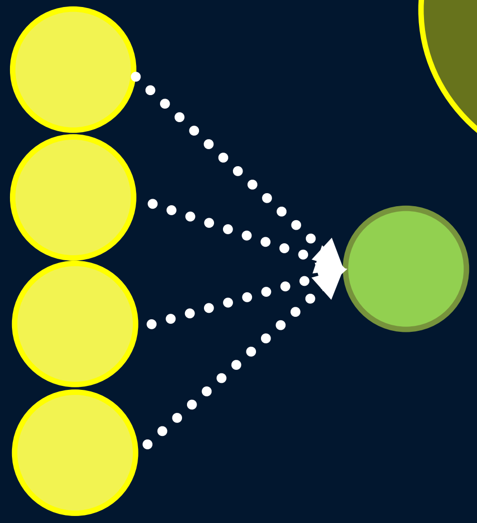
流量分析

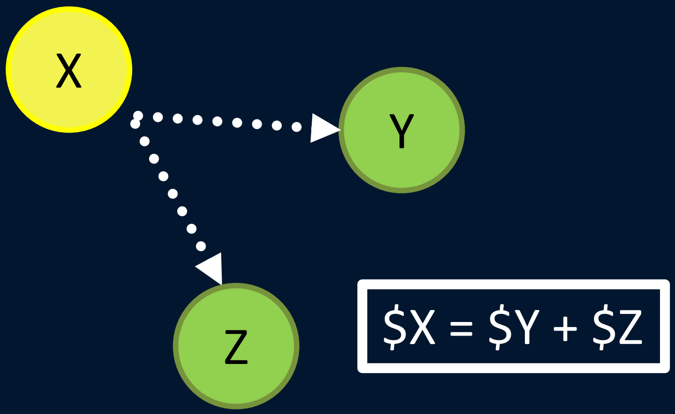
旁道攻擊

模式識別

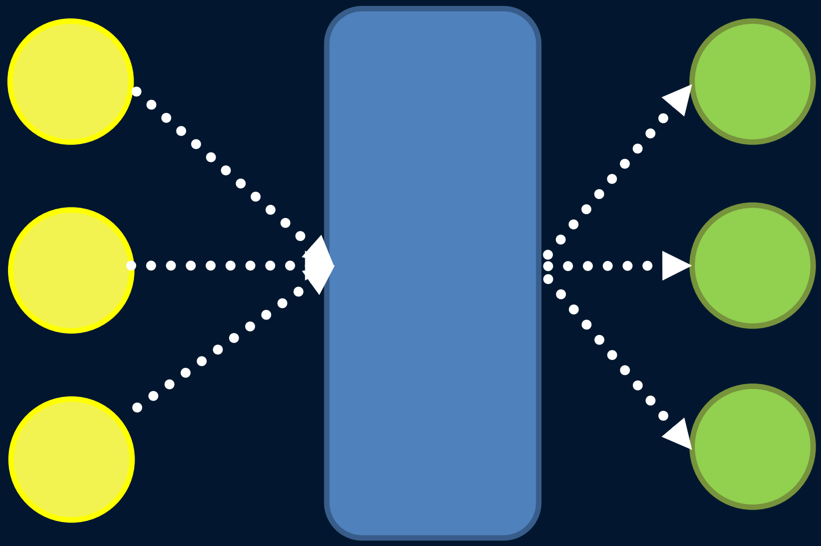
金融
安全





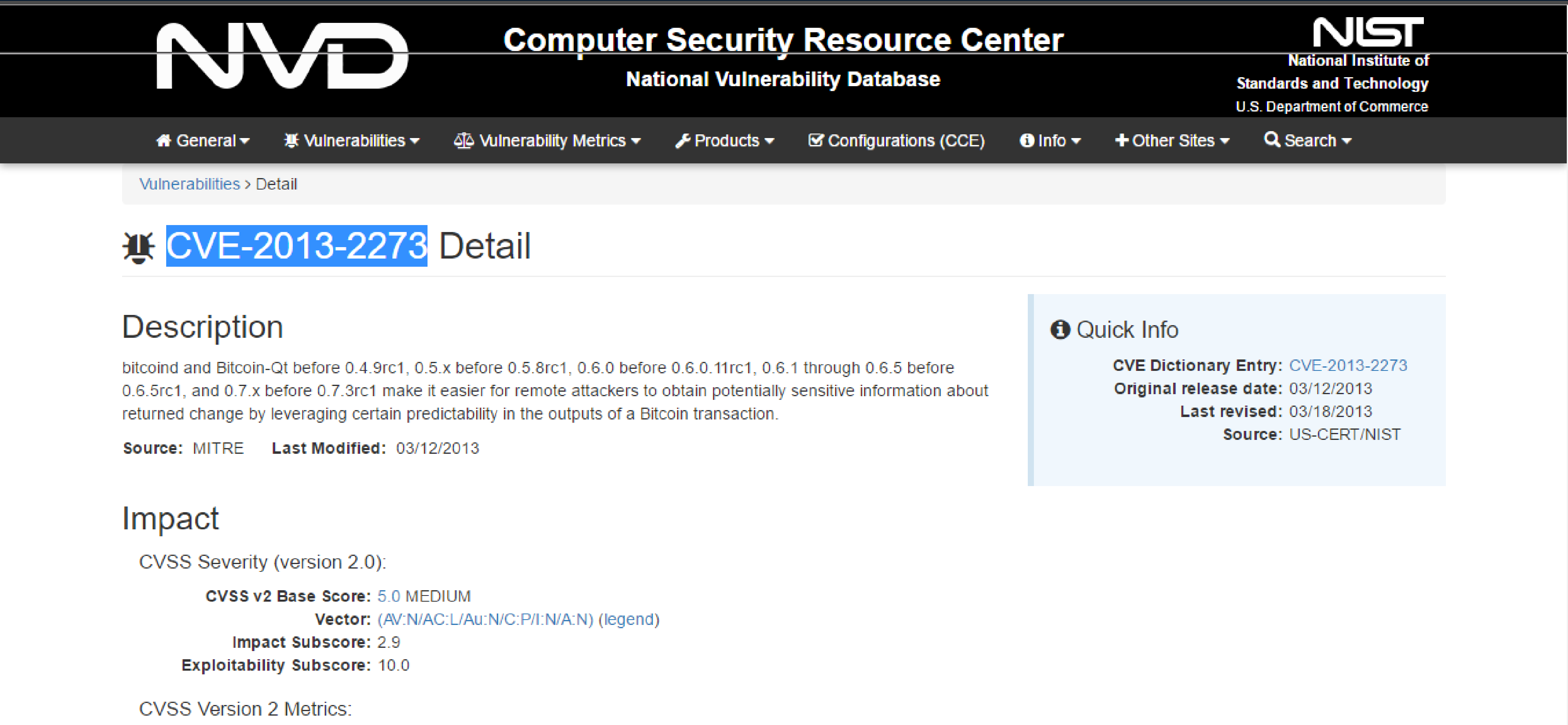


$X = $Y + $Z



CVE-2013-2273

金融
安全



CVE-2013-2273 Detail

Description

bitcoind and Bitcoin-Qt before 0.4.9rc1, 0.5.x before 0.5.8rc1, 0.6.0 before 0.6.0.11rc1, 0.6.1 through 0.6.5 before 0.6.5rc1, and 0.7.x before 0.7.3rc1 make it easier for remote attackers to obtain potentially sensitive information about returned change by leveraging certain predictability in the outputs of a Bitcoin transaction.

Source: MITRE **Last Modified:** 03/12/2013

Quick Info

CVE Dictionary Entry: CVE-2013-2273
Original release date: 03/12/2013
Last revised: 03/18/2013
Source: US-CERT/NIST

Impact

CVSS Severity (version 2.0):

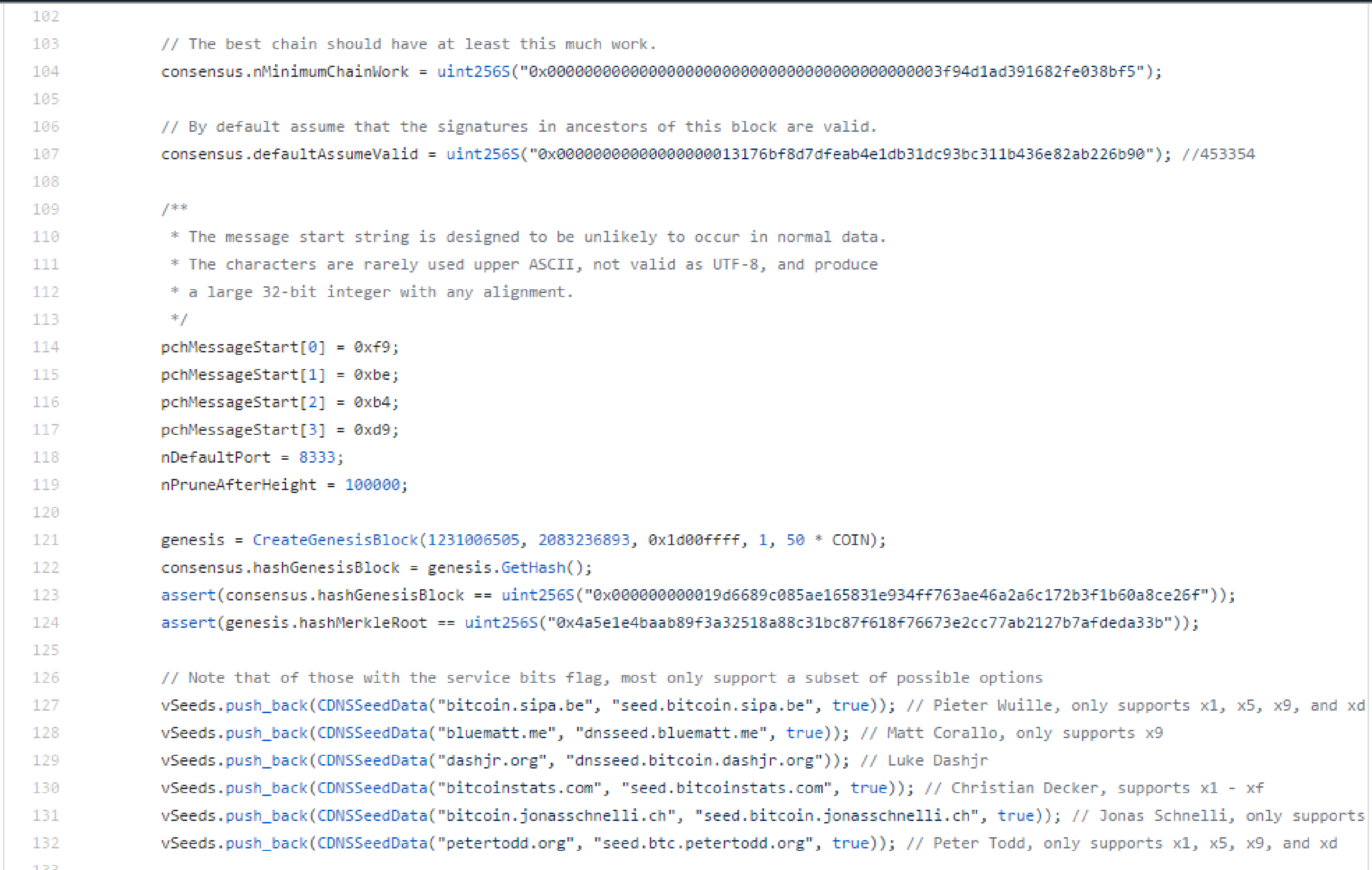
CVSS v2 Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

破碎的子圖探勘

Seed (Domain Name)

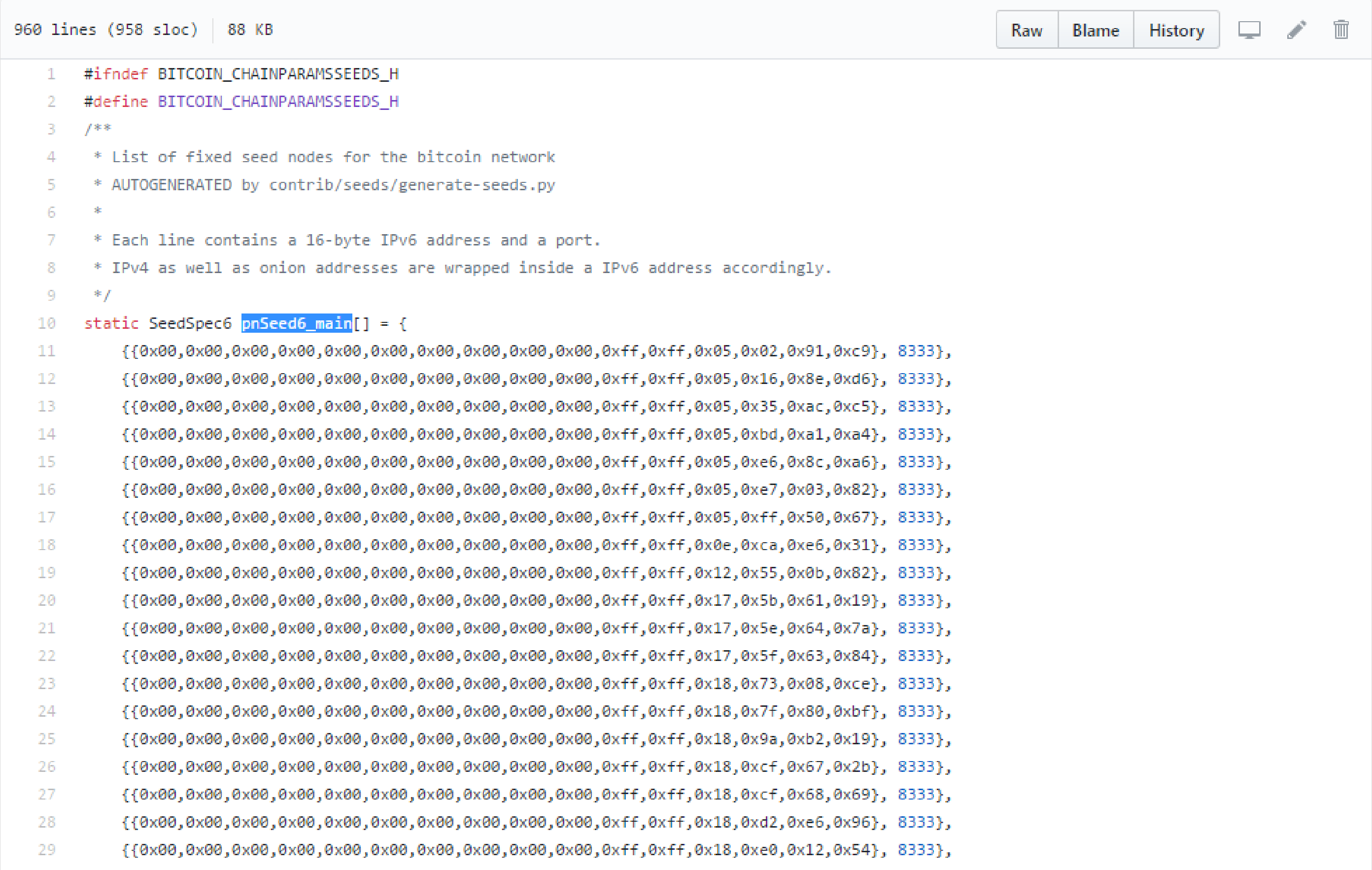
網路安全



```
        // The best chain should have at least this much work.
        consensus.nMinimumChainWork = uint256S("0x0000000000000000000000000000000000000000003f94d1ad391682fe038bf5");

        // By default assume that the signatures in ancestors of this block are valid.
        consensus.defaultAssumeValid = uint256S("0x00000000000000000013176bf8d7dfeab4e1db31dc93bc311b436e82ab226b90"); //453354

        /**
         * The message start string is designed to be unlikely to occur in normal data.
         * The characters are rarely used upper ASCII, not valid as UTF-8, and produce
         * a large 32-bit integer with any alignment.
         */
        pchMessageStart[0] = 0xf9;
        pchMessageStart[1] = 0xbe;
        pchMessageStart[2] = 0xb4;
        pchMessageStart[3] = 0xd9;
        nDefaultPort = 8333;
        nPruneAfterHeight = 100000;

        genesis = CreateGenesisBlock(1231006505, 2083236893, 0x1d00ffff, 1, 50 * COIN);
        consensus.hashGenesisBlock = genesis.GetHash();
        assert(consensus.hashGenesisBlock == uint256S("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f"));
        assert(genesis.hashMerkleRoot == uint256S("0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"));

        // Note that of those with the service bits flag, most only support a subset of possible options
        vSeeds.push_back(CDNSSeedData("bitcoin.sipa.be", "seed.bitcoin.sipa.be", true)); // Pieter Wuille, only supports x1, x5, x9, and xd
        vSeeds.push_back(CDNSSeedData("bluematt.me", "dnsseed.bluematt.me", true)); // Matt Corallo, only supports x9
        vSeeds.push_back(CDNSSeedData("dashjr.org", "dnsseed.bitcoin.dashjr.org")); // Luke Dashjr
        vSeeds.push_back(CDNSSeedData("bitcoinstats.com", "seed.bitcoinstats.com", true)); // Christian Decker, supports x1 - xf
        vSeeds.push_back(CDNSSeedData("bitcoin.jonasschnelli.ch", "seed.bitcoin.jonasschnelli.ch", true)); // Jonas Schnelli, only supports
        vSeeds.push_back(CDNSSeedData("petertodd.org", "seed.btc.petertodd.org", true)); // Peter Todd, only supports x1, x5, x9, and xd
```

Seed (IP:Port)

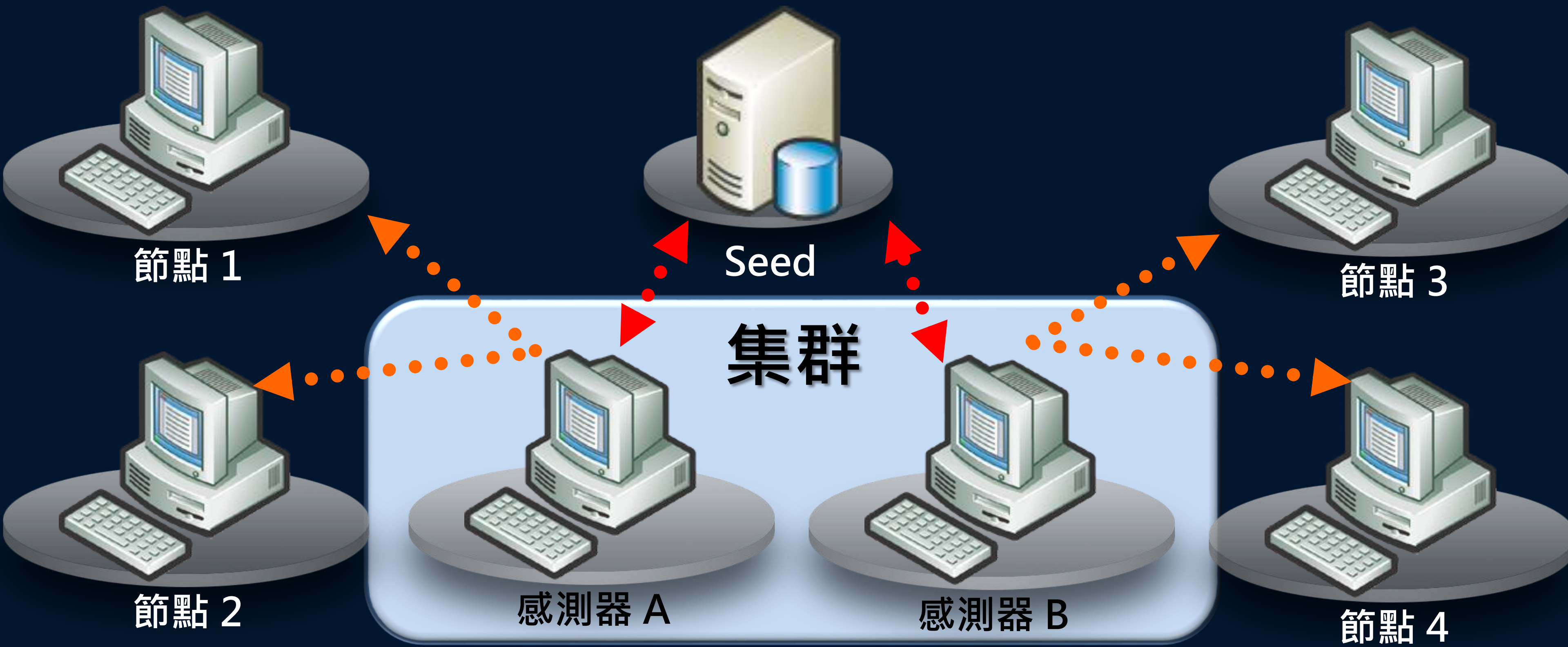
網路
安全



```
#ifndef BITCOIN_CHAINPARAMSSEEDS_H
#define BITCOIN_CHAINPARAMSSEEDS_H
/**
 * List of fixed seed nodes for the bitcoin network
 * AUTOGENERATED by contrib/seeds/generate-seeds.py
 *
 * Each line contains a 16-byte IPv6 address and a port.
 * IPv4 as well as onion addresses are wrapped inside a IPv6 address accordingly.
 */
static SeedSpec6 pnSeed6_main[] = {
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x05,0x02,0x91,0xc9}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x05,0x16,0x8e,0xd6}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x05,0x35,0xac,0xc5}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x05,0xbd,0xa1,0xa4}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x05,0xe6,0x8c,0xa6}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x05,0xe7,0x03,0x82}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x05,0xff,0x50,0x67}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x0e,0xca,0xe6,0x31}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x12,0x55,0x0b,0x82}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x17,0x5b,0x61,0x19}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x17,0x5e,0x64,0x7a}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x17,0x5f,0x63,0x84}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x18,0x73,0x08,0xce}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x18,0x7f,0x80,0xbf}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x18,0x9a,0xb2,0x19}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x18,0xcf,0x67,0x2b}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x18,0xcf,0x68,0x69}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x18,0xd2,0xe6,0x96}, 8333},
    {{0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xff,0xff,0x18,0xe0,0x12,0x54}, 8333},
```

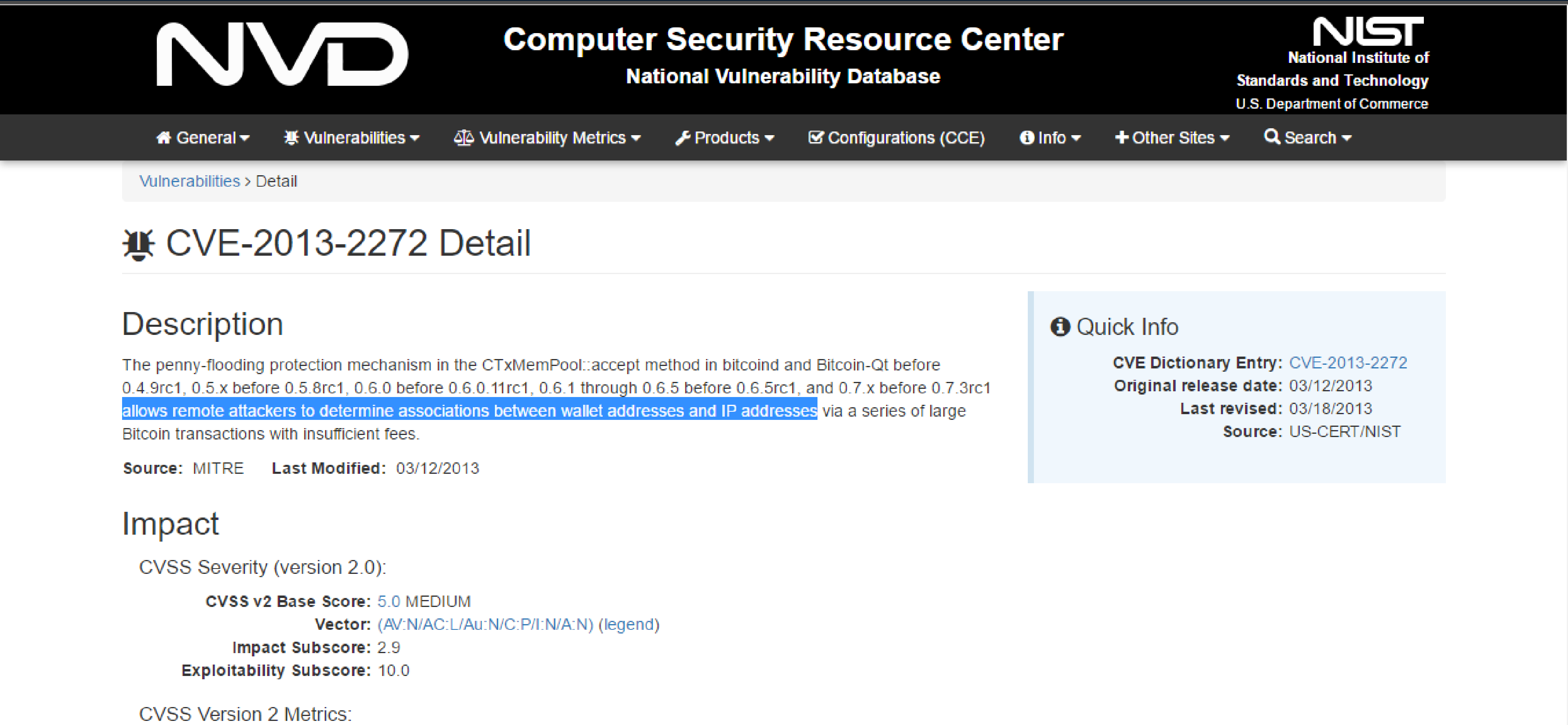
Bitcoin 感測器網路

網路
安全



CVE-2013-2272

網路安全


NVD
Computer Security Resource Center
National Vulnerability Database
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
General
Vulnerabilities
Vulnerability Metrics
Products
Configurations (CCE)
Info
Other Sites
Search
Vulnerabilities > Detail

CVE-2013-2272 Detail

Description

The penny-flooding protection mechanism in the CTxMemPool::accept method in bitcoind and Bitcoin-Qt before 0.4.9rc1, 0.5.x before 0.5.8rc1, 0.6.0 before 0.6.0.11rc1, 0.6.1 through 0.6.5 before 0.6.5rc1, and 0.7.x before 0.7.3rc1 allows remote attackers to determine associations between wallet addresses and IP addresses via a series of large Bitcoin transactions with insufficient fees.

Source: MITRE **Last Modified:** 03/12/2013

Quick Info

CVE Dictionary Entry: CVE-2013-2272
Original release date: 03/12/2013
Last revised: 03/18/2013
Source: US-CERT/NIST

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

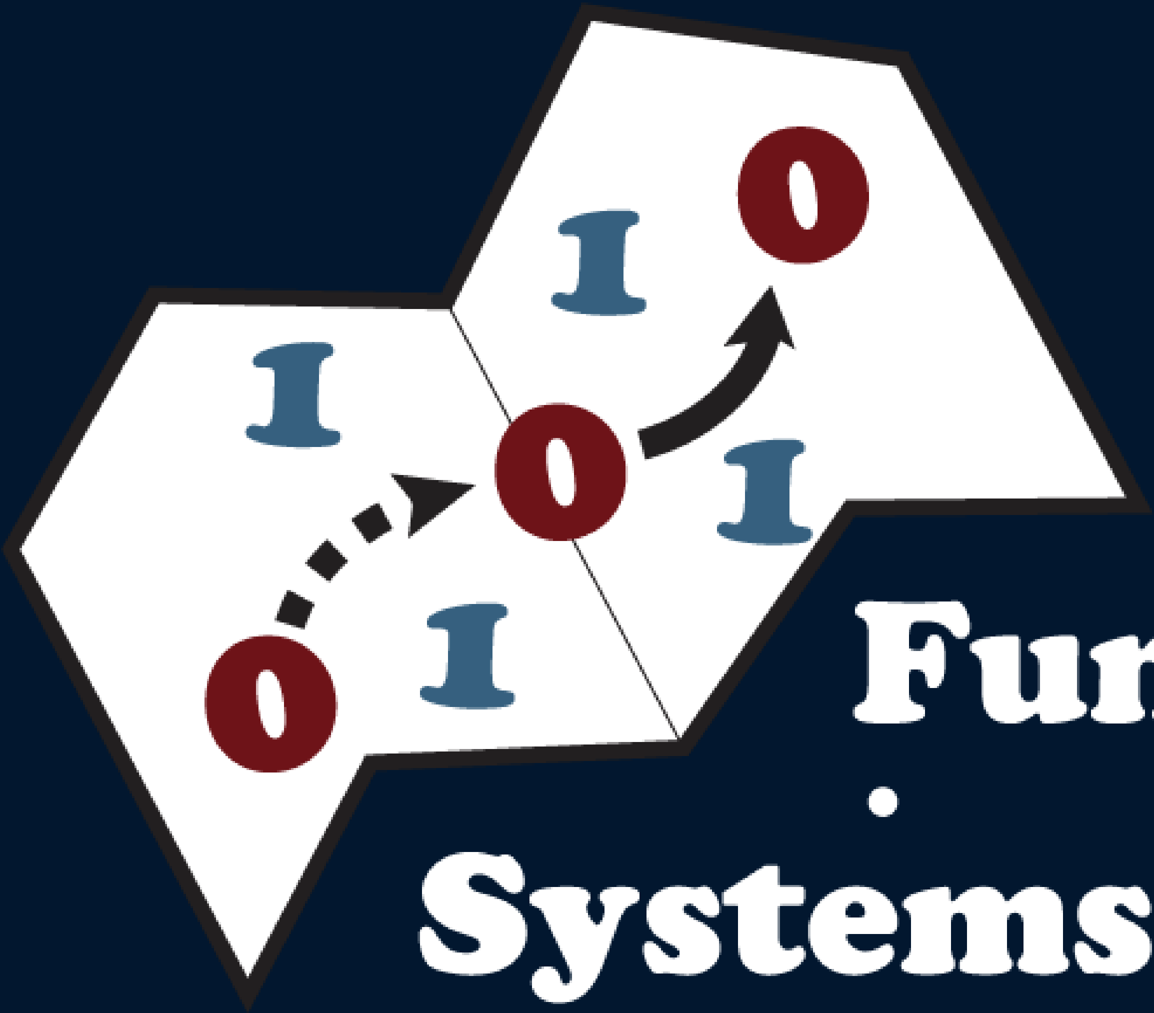
河量數據

緊盯 關鍵節點

交易所 網路服務業者 網域伺服器

交易所 網路服務業者 網域伺服器

剝洋蔥



Funny
•
Systems

法泥系統 » Funny Systems

共同 **研究** » 保障交易所 & 智能合約

共同 **開發** » 反洗錢, 交易追蹤, 匿名識別

不用閃開　跟專業一起來

Bitcoin@Funny.Systems

SmartContract@Funny.Systems

問題·討論

Q&A