Common Vulnerabilities and Exposures

CVE	Announced	Affects	Severity	Attack is...	Flaw	Net
Pre-BIP protocol changes	n/a	All Bitcoin clients	Netsplit[1]	Implicit[2]	Various hardforks and softforks	100%
CVE-2010-5137	2010-07-28	wxBitcoin and bitcoind	DoS[3]	Easy	OP_LSHIFT crash	100%
CVE-2010-5141	2010-07-28	wxBitcoin and bitcoind	Theft[4]	Easy	OP_RETURN could be used to spend any output.	100%
CVE-2010-5138	2010-07-29	wxBitcoin and bitcoind	DoS[3]	Easy	Unlimited SigOp DoS	100%
CVE-2010-5139	2010-08-15	wxBitcoin and bitcoind	Inflation[5]	Easy	Combined output overflow	100%
CVE-2010-5140	2010-09-29	wxBitcoin and bitcoind	DoS[3]	Easy	Never confirming transactions	100%
CVE-2011-4447	2011-11-11	wxBitcoin and bitcoind	Exposure[6]	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[1]	Very hard	Transaction overwriting	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-1909.html)
CVE-2012-1910	2012-03-17	bitcoind & Bitcoin-Qt for Windows	Unknown[7]	Hard	Non-thread safe MingW exceptions	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-1910.html)
BIP 0016	2012-04-01	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softfork: P2SH	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/BIP-0016.html)

CVE-2012-2459	2012-05-14	bitcoind and Bitcoin-Qt	Netsplit[1]	Easy	Block hash collision (via merkle root)	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-2459.html)
CVE-2012-3789	2012-06-20	bitcoind and Bitcoin-Qt	DoS[3]	Easy	(Lack of) orphan txn resource limits	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20123789)
CVE-2012-4682		bitcoind and Bitcoin-Qt	DoS[3]			100% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-4682.html)
CVE-2012-4683	2012-08-23	bitcoind and Bitcoin-Qt	DoS[3]	Easy	Targeted DoS by CPU exhaustion using alerts	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-4683.html)
CVE-2012-4684	2012-08-24	bitcoind and Bitcoin-Qt	DoS[3]	Easy	Network-wide DoS using malleable signatures in alerts	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20124684)
CVE-2013-2272	2013-01-11	bitcoind and Bitcoin-Qt	Exposure[6]	Easy	Remote discovery of node's wallet addresses	99.99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132272)
CVE-2013-2273	2013-01-30	bitcoind and Bitcoin-Qt	Exposure[6]	Easy	Predictable change output	99.99% (http://luke.dashjr.

						org/programs/bitcoin/files/charts/security.html?20132273)
CVE-2013-2292	2013-01-30	bitcoind and Bitcoin-Qt	DoS[3]	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[3]	Easy	Continuous hard disk seek	99.99% (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[8]	Miners[9]	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[1]	Hard	Inconsistent BDB lock limit interactions	99.99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20133220)
BIP 0034	2013-03-25	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softfork: Height in coinbase	100% (http://luke.dashjr.org/programs/bitcoin/files/charts/BIP-0034.html)
BIP 0050	2013-05-15	All Bitcoin clients	Netsplit[1]	Implicit[2]	Hard fork to remove txid limit protocol rule	99.99% (http://luke.dashjr.org/progr

						ams/bitcoin/files/charts/security.html?50)
CVE-2013-4627	2013-06-??	bitcoind and Bitcoin-Qt	DoS[3]	Easy	Memory exhaustion with excess tx message data	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?2013462 7)
CVE-2013-4165	2013-07-20	bitcoind and Bitcoin-Qt	Theft[10]	Local	Timing leak in RPC authentication	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?2013416 5)
CVE-2013-5700	2013-09-04	bitcoind and Bitcoin-Qt 0.8.x	DoS[3]	Easy	Remote p2p crash via bloom filters	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?2013570 0)
CVE-2014-0160	2014-04-07	Anything using OpenSSL for TLS	Unknown[7]	Easy	Remote memory leak via payment protocol	Unknown
CVE-2015-3641 (https://bitcoincore.org/en/2024/07/03/disclose_receive_buffer_oom/)	2014-07-07	bitcoind and Bitcoin-Qt prior to 0.10.2	DoS[3]	Easy	OOM via p2p	99.9% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?2013570 0)
BIP 66	2015-02-13	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softfork: Strict DER signatures	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?66)

BIP 65	2015-11-12	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softfork: OP_CHECKLOCKTIMEVERIFY	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?65)
BIPs 68, 112 & 113	2016-04-11	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softforks: Rel locktime, CSV & MTP locktime	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?68)
CVE-2015-6031	2015-09-15	MiniUPnPc Bitcoin Core/Knots prior to 0.11.2	Anything	LAN	Buffer overflow	
BIPs 141, 143 & 147	2016-10-27	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softfork: Segwit	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?141)
CVE-2016-8889	2016-10-27	Bitcoin Knots GUI 0.11.0 - 0.13.0	Exposure	Hard	Debug console history storing sensitive info	100%
CVE-2017-9230	?	Bitcoin	?	?	ASICBoost	0%
BIP 148	2017-03-12	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softfork: Segwit UASF	?
CVE-2017-12842	2018-06-09				No commitment to block merkle tree depth	
CVE-2016-10724 (https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-July/016189.html)	2018-07-02	bitcoind and Bitcoin-Qt prior to 0.13.0	DoS[3]	Keyholders[11]	Alert memory exhaustion	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20161072 4)
TBD (https://bitcoin	2024-07-03	Bitcoin Core/Knots	DoS[3]	Easy	OOM via fake block headers	

core.org/en/2024/07/03/disclose-header-spam/)		prior to 0.15.0				
CVE-2016-10725 (https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-July/016189.html)	2018-07-02	bitcoind and Bitcoin-Qt prior to 0.13.0	DoS[3]	Keyholders[11]	Final alert cancellation	99% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20161072 4)
CVE-2018-17144	2018-09-17	bitcoind and Bitcoin-Qt prior to 0.16.3	Inflation[5]	Miners[9]	Missing check for duplicate inputs	80% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20181714 4)
CVE-2018-20587 (https://medium.com/@lukedashjr/cve-2018-20587-advisory-and-full-disclosure-a3105551e78b)	2019-02-08	Bitcoin Knots prior to 0.17.1, and all current Bitcoin Core releases	Theft[10]	Local	No alert for RPC service binding failure	<1% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20182058 7)
CVE-2017-18350	2019-06-22	bitcoind and Bitcoin-Qt prior to 0.15.1	Unknown	Varies[12]	Buffer overflow from SOCKS proxy	94% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20171835 0)
CVE-2018-20586	2019-06-22	bitcoind and Bitcoin-Qt prior to 0.17.1	Deception	RPC access	Debug log injection via unauthenticated RPC	77% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20182058 6)

TBD (https://bitcoincore.org/en/2024/07/03/disclose-orphan-dos/)	2024-07-03	Bitcoin Core/Knots prior to 0.18.0	DoS	Easy	Orphan transaction CPU tieup	
CVE-2019-12998 (https://lists.linuxfoundation.org/pipermail/lightning-dev/2019-September/002174.html)	2019-08-30	c-lightning prior to 0.7.1	Theft	Easy	Missing check of channel funding UTXO	
CVE-2019-12999 (https://lists.linuxfoundation.org/pipermail/lightning-dev/2019-September/002174.html)	2019-08-30	lnd prior to 0.7	Theft	Easy	Missing check of channel funding UTXO amount	
CVE-2019-13000 (https://lists.linuxfoundation.org/pipermail/lightning-dev/2019-September/002174.html)	2019-08-30	eclair prior to 0.3	Theft	Easy	Missing check of channel funding UTXO	
TBD (https://bitcoincore.org/en/2024/07/03/disclose-inv-buffer-blowup/)	2024-07-03	Bitcoin Core/Knots prior to 0.20.0	DoS	Easy	Network buffer OOM	
TBD (https://bitcoincore.org/en/2024/07/03/disclose-getdata-cpu/)	2024-07-03	Bitcoin Core/Knots prior to 0.20.0	CPU usage	Easy	Infinite loop via p2p	
TBD (https://bitcoin	2024-07-03	Bitcoin Core/Knots	DoS	Recipient[13]	OOM via malicious BIP72 URI	

core.org/en/2024/07/03/disclose-bip70-crash/)		prior to 0.20.0				
CVE-2020-14199	2020-06-03	Trezor and others	Theft	Social[14]	Double-signing can enable unintended fees	
CVE-2018-17145 (https://invdos.net/)	2020-09-09	Bitcoin Core prior to 0.16.2 Bitcoin Knots prior to 0.16.1 Bcoin prior to 1.0.2 Btcd prior to 0.21.0	DoS[3]	Easy	p2p memory blow-up	87% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20181714 5)
CVE-2020-26895	2020-10-08	lnd prior to 0.10	Theft	Easy	Missing low-S normalization for HTLC signatures	
CVE-2020-26896	2020-10-08	lnd prior to 0.11	Theft	Varies[15]	Invoice preimage extraction via forwarded HTLC	
CVE-2020-14198 (https://bitcoincore.org/en/2024/07/03/disclose-unbounded-banlist/)		Bitcoin Core 0.20.1	DoS[3]	Easy	Remote DoS	93% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20201419 8)
TBD (https://bitcoincore.org/en/2024/07/03/disclose-timestamp-overflow/)	2024-07-03	Bitcoin Core/Knots prior to 0.20.2	Netsplit[1]	Varies	Adjusted time manipulation	
CVE-2021-3401	2021-02-01	Bitcoin Core GUI prior to 0.19.0 Bitcoin Knots GUI prior to 0.18.1	Theft	Hard	Qt5 remote execution	64% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20213401)
CVE-2024-52917 (https://bitcoincore.org/en/2024/07/31/discl	2024-07-31	Bitcoin Core/Knots prior to 22.0 with UPnP enabled	DoS	Local	OOM via LAN spam	

ose-upnp-oom/)						
CVE-2024-52919 (https://bitcoincore.org/en/2024/07/31/disclose-addrman-int-overflow/)	2024-07-31	Bitcoin Core/Knots prior to 22.0	DoS	Easy	OOM via p2p spam	
CVE-2021-31876	2021-05-06	Various wallets				
CVE-2021-41591	2021-10-04	Lightning software				
CVE-2021-41592	2021-10-04	Lightning software				
CVE-2021-41593	2021-10-04	Lightning software				
BIPs 341-343	2021-11-13	All Bitcoin nodes	Fake Conf[8]	Miners[9]	Softfork: Taproot	57% (http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?343)
CVE-2022-31246 (https://github.com/spesmilo/electrum/security/advisories/GHSA-4fh4-hx35-r355)	2022-06-07	Electrum 2.1 until before 4.2.2	Theft	Social		
CVE-2023-50428	2023	Bitcoin core 0.9 and newer (not fixed) Bitcoin Knots 0.9 - 23.0	DoS[3]	Easy	Bypass of datacarriersize limit using OP_FALSE,OP_IF	
CVE-2024-34149	2024-03-30	Bitcoin Core 0.21.1 and newer (not fixed) Bitcoin Knots	DoS[3]	Easy	Script size limit not enforced for Tapscript	

		0.21.1 - 0.23.0				
CVE-2019-25220 (https://bitcoincore.org/en/2024/09/18/disclose-headers-oom/)	2024-09-18	Bitcoin Core prior to 24.0.1 (Bitcoin Knots unaffected)	DoS[3]		Memory DoS due to headers spam	
CVE-2024-52921 (https://bitcoincore.org/en/2024/10/08/disclose-mutated-blocks-hindering-propagation/)	2024-10-09	Bitcoin Core/Knots prior to 25.0			Hindered block propagation due to mutated blocks	
TBD (https://bitcoincore.org/en/2024/10/08/disclose-large-inv-to-send/)	2024-10-09	Bitcoin Core/Knots prior to 25.0			DoS due to inv-to-send sets growing too large	
CVE-2024-35202 (https://bitcoincore.org/en/2024/10/08/disclose-blocktxn-crash/)	2024-10-09	Bitcoin Core/Knots prior to 25.0				
CVE-2024-52922 (https://bitcoincore.org/en/2024/11/05/cb-stall-hindering-propagation/)	2024-11-05	Bitcoin Core/Knots prior to 25.1				

1. Attacker can create multiple views of the network, enabling double-spending with over 1 confirmation
2. This is a protocol "hard-fork" that old clients will reject as invalid and must therefore not be used.
3. Attacker can disable some functionality, for example by crashing clients
4. Attacker can take coins outside known network rules
5. Attacker can create coins outside known network rules
6. Attacker can access user data outside known acceptable methods

7. Extent of possible abuse is unknown
8. Attacker can double-spend with 1 confirmation
9. Attacking requires mining block(s)
10. Local attacker could potentially determine the RPC passphrase via a timing sidechannel.
11. Attacking requires signing with the publicly-disclosed alert key
12. Depends on software configuration
13. Can only be exploited by the recipient the victim intends to pay
14. User must be tricked into cooperating (social engineering)
15. Depends on node configuration, only affects routable merchants, requires external knowledge of receiver's invoices and/or luck to identify receiver, only works against single-shot HTLCs (legacy or MPP)

CVE-2010-5137

Date: 2010-07-28
Summary: OP_LSHIFT crash
Fix Deployment: 100%

Affected		Fix
bitcoind wxBitcoin	* - 0.3.4	0.3.5

On July 28 2010, two bugs were discovered and demonstrated on the test network. One caused bitcoin to crash on some machines when processing a transaction containing an OP_LSHIFT. This was never exploited on the main network, and was fixed by Bitcoin version 0.3.5.

After these bugs were discovered, many currently-unused script words were disabled for safety.

References

- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5137)

CVE-2010-5141

Date: 2010-07-28
Summary: ?
Fix Deployment: 100%

Affected		Fix
bitcoind wxBitcoin	* - 0.3.4	0.3.5

On July 28 2010, two bugs were discovered and demonstrated on the test network. One exploited a bug in the transaction handling code and allowed an attacker to spend coins that they did not own. This was never exploited on the main network, and was fixed by Bitcoin version 0.3.5.

After these bugs were discovered, many currently-unused script words were disabled for safety.

References

- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5141)

CVE-2010-5138

Date: 2010-07-29
Summary: Unlimited SigOp DoS
Fix Deployment: 100%

Affected		Fix
bitcoind wxBitcoin	* - 0.3.?	0.3.?

On July 29 2010, it was discovered that block 71036 (http://blockexplorer.com/block/00000000000997f9fd2fe1ee376293ef8c42ad09193a5d2086dddf8e5c426b56) contained several transactions with a ton of OP_CHECKSIG commands. There should only ever be one such command. This caused every node to do extra unnecessary work, and it could have been used as a denial-of-service attack. A new version of Bitcoin was quickly released. The new version did not cause a fork on the main network, though it did cause one on the test network (where someone had played around with the attack more).

References

- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5138)

CVE-2010-5139

Main article: CVE-2010-5139

Date: 2010-08-15
Summary: Combined output overflow
Fix Deployment: 100%

Affected		Fix
bitcoind wxBitcoin	* - 0.3.10	0.3.11

On August 15 2010, it was discovered (http://bitcointalk.org/index.php?topic=822.0) that block 74638 contained a transaction that created over 184 billion bitcoins for two different addresses. This was possible because the code used for checking transactions before including them in a block didn't account for the case of outputs so large that they overflowed when summed. A new version was published within a few hours of the discovery. The block chain had to be forked. Although many unpatched nodes continued to build on the "bad" block chain, the "good" block chain overtook it at a block height of 74691. The bad transaction no longer exists for people using the longest chain.

The block and transaction:

```
CBlock(hash=0000000000790ab3, ver=1, hashPrevBlock=0000000000606865, hashMerkleRoot=618eba,
nTime=1281891957, nBits=1c00800e, nNonce=28192719, vtx=2)
  CTransaction(hash=012cd8, ver=1, vin.size=1, vout.size=1, nLockTime=0)
    CTxIn(COutPoint(000000, -1), coinbase 040e80001c028f00)
    CTxOut(nValue=50.51000000, scriptPubKey=0x4F4BA55D1580F8C3A8A2C7)
  CTransaction(hash=1d5e51, ver=1, vin.size=1, vout.size=2, nLockTime=0)
    CTxIn(COutPoint(237fe8, 0), scriptSig=0xA87C02384E1F184B79C6AC)
    CTxOut(nValue=92233720368.54275808, scriptPubKey=OP_DUP OP_HASH160 0xB7A7)
    CTxOut(nValue=92233720368.54275808, scriptPubKey=OP_DUP OP_HASH160 0x1512)
  vMerkleTree: 012cd8 1d5e51 618eba

Block hash: 0000000000790ab3f22ec756ad43b6ab569abf0bddeb97c67a6f7b1470a7ec1c
Transaction hash: 1d5e512a9723cbef373b970eb52f1e9598ad67e7408077a82fdac194b65333c9
```

References

- Discovery (https://bitcointalk.org/index.php?topic=822.0)
- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5139)

CVE-2010-5140

Date: 2010-09-29
Summary: Never confirming transactions
Fix Deployment: 100%

Affected		Fix
bitcoind wxBitcoin	* - 0.3.12	0.3.13

Around September 29, 2010, people started reporting (https://bitcointalk.org/index.php?topic=1306.0) that their sent transactions would not confirm. This happened because people modified Bitcoin to send sub-0.01 transactions without any fees. A 0.01 fee was at that time required by the network for such transactions (essentially prohibiting them), so the transactions remained at 0 confirmations forever. This became a more serious issue because Bitcoin would send transactions using bitcoins gotten from transactions with 0 confirmations, and these resulting transactions would also never confirm. Because Bitcoin tends to prefer sending smaller coins, these invalid transactions quickly multiplied, contaminating the wallets of everyone who received them.

Bitcoin was changed to only select coins with at least 1 confirmation. The remaining sub-0.01 transactions were cleared by generators who modified their version of Bitcoin to not require the micropayment fee. It took a while for everything to get cleared, though, because many of the intermediate transactions had been forgotten by the

network by this point and had to be rebroadcast by the original senders.

References

- Initial reports (https://bitcointalk.org/index.php?topic=1306.0)
- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5140)

CVE-2011-4447

Date: 2011-11-11
Summary: Wallet non-encryption
Fix Deployment: 100%

Affected		Fix
bitcoind wxBitcoin	0.4.0 - 0.4.1rc6	0.4.1 0.5.0

References

- Announcement (https://bitcointalk.org/index.php?topic=51604.0)
- Finding (https://bitcointalk.org/index.php?topic=51474.0)
- 0.5.0 (http://bitcoin.org/releases/2011/11/21/v0.5.0.html)
- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4447)

CVE-2012-1909

Date: 2012-03-07
Summary: Transaction overwriting
Fix Deployment: 100%

Affected		Fix
Bitcoin protocol	Before March 15th, 2012	BIP 30
Bitcoin-Qt bitcoind	* - 0.4.4rc2 0.5.0rc1 - 0.5.0.4rc2 0.5.1rc1 - 0.5.3rc2 0.6.0rc1 - 0.6.0rc2	0.4.4 0.5.0.4 0.5.3 0.6.0rc3
wxBitcoin	ALL	NONE

References

- Announcement (https://bitcointalk.org/index.php?topic=67738.0)
- Fix (https://en.bitcoin.it/wiki/BIP_0030)
- Gentoo bug tracker (https://bugs.gentoo.org/show_bug.cgi?id=407793)

- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1909)

CVE-2012-1910

Date: 2012-03-17
Summary: Non-thread safe MingW exceptions
Fix Deployment: 100%

Affected		Fix
bitcoind for Windows Bitcoin-Qt for Windows	0.5.0rc1 - 0.5.0.4 0.5.1rc1 - 0.5.3.0 0.6.0rc1 - 0.6.0rc3	0.5.0.5 0.5.3.1 0.5.4 0.6.0rc4

References

- Announcement (https://bitcointalk.org/index.php?topic=69120.0)
- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1910)
- Full disclosure (http://gavintech.blogspot.com/2012/03/full-disclosure-bitcoin-qt-on-windows.html)

BIP-0016

Date: 2012-04-01
Summary: Mandatory P2SH protocol update
Deployment: 100%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.4 0.5.0rc1 - 0.5.0.5 0.5.1rc1 - 0.5.3 0.6.0rc1	0.4.5 0.5.0.6 0.5.4rc1 0.6.0rc2
wxBitcoin	ALL	NONE

References

- BIP 0016

CVE-2012-2459

Date: 2012-05-14
Summary: Block hash collision (via merkle tree)
Fix Deployment: 100%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.6rc1 0.5.0rc1 - 0.5.5rc1 0.6.0rc1 - 0.6.0.7rc1 0.6.1rc1 - 0.6.1rc1	0.4.6 0.5.5 0.6.0.7 0.6.1rc2

Block hash collisions can easily be made by duplicating transactions in the merkle tree. Such a collision is invalid, but if recorded (as Bitcoin-Qt and bitcoind prior to 0.6.1 did) would prevent acceptance of the legitimate block with the same hash. This could be used to fork the blockchain, including deep double-spend attacks.

References

- Announcement (https://bitcointalk.org/?topic=81749)
- Gentoo bug tracker (https://bugs.gentoo.org/show_bug.cgi?id=415973)
- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2459)
- Full Disclosure (https://bitcointalk.org/?topic=102395)

CVE-2012-3789

Main article: CVE-2012-3789

Date: 2012-06-20
Summary: (Lack of) orphan txn resource limits
Fix Deployment: 100%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.7rc2 0.5.0rc1 - 0.5.6rc2 0.6.0rc1 - 0.6.0.8rc2 0.6.1rc1 - 0.6.2.2	0.4.7rc3 0.5.6rc3 0.6.0.9rc1 0.6.3rc1

References

- CVE-2012-3789
- 0.6.3rc1 Announcement (https://bitcointalk.org/?topic=88734)
- US-CERT/NIST (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3789)

CVE-2012-4682

Date:
Summary:
Fix Deployment: 100%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.7rc2 0.5.0rc1 - 0.5.6rc2 0.6.0rc1 - 0.6.0.8rc2 0.6.1rc1 - 0.6.2.2	0.4.7rc3 0.5.6rc3 0.6.0.9rc1 0.6.3rc1

References

- CVE-2012-4682
- Gentoo bug (https://bugs.gentoo.org/show_bug.cgi?id=435216)

CVE-2012-4683

Main article: CVE-2012-4683

Date: 2012-08-23
Summary: Targeted DoS by CPU exhaustion using alerts
Fix Deployment: 100%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.7rc2 0.5.0rc1 - 0.5.6rc2 0.6.0rc1 - 0.6.0.8rc2 0.6.1rc1 - 0.6.2.2	0.7.0

References

- CVE-2012-4683
- Announcement (https://bitcointalk.org/index.php?topic=148038.0)
- Gentoo bug (https://bugs.gentoo.org/show_bug.cgi?id=435216)

CVE-2012-4684

Main article: CVE-2012-4684

Date: 2012-08-24
Summary: Network-wide DoS using malleable signatures in alerts
Fix Deployment: 100%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.7rc2 0.5.0rc1 - 0.5.6rc2 0.6.0rc1 - 0.6.0.8rc2 0.6.1rc1 - 0.6.2.2 - 0.6.3rc1	0.7.0

References

- CVE-2012-4684
- Announcement (https://bitcointalk.org/index.php?topic=148109.0)

CVE-2013-2272

Date: 2013-01-11
Summary: Remote discovery of node's wallet addresses
Fix Deployment: 99.99%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.8rc4 0.5.0rc1 - 0.5.7 0.6.0rc1 - 0.6.0.10rc4 0.6.1rc1 - 0.6.4rc4 0.7.0rc1 - 0.7.2	0.4.9rc1 0.5.8rc1 0.6.0.11rc1 0.6.5rc1 0.7.3rc1

References

- Announcement (https://bitcointalk.org/?topic=135856)
- Gentoo bug (https://bugs.gentoo.org/show_bug.cgi?id=462046)

CVE-2013-2273

Date: 2013-01-30
Summary: Predictable change output
Fix Deployment: 99.99%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.8rc4 0.5.0rc1 - 0.5.7 0.6.0rc1 - 0.6.0.10rc4 0.6.1rc1 - 0.6.4rc4 0.7.0rc1 - 0.7.2	0.4.9rc1 0.5.8rc1 0.6.0.11rc1 0.6.5rc1 0.7.3rc1

References

- Gentoo bug (https://bugs.gentoo.org/show_bug.cgi?id=462046)

CVE-2013-2292

Date: 2013-01-30
Summary: A transaction that takes at least 3 minutes to verify
Fix Deployment: 0%

Affected		Fix
Bitcoin-Qt bitcoind	All versions	No fix yet

References

- CVE-2013-2292
- Announcement (https://bitcointalk.org/?topic=140078)
- Gentoo bug (https://bugs.gentoo.org/show_bug.cgi?id=462046)

CVE-2013-2293

Main article: CVE-2013-2293

Date: 2013-02-14
Summary: Continuous hard disk seek
Fix Deployment: 99.99%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.7.3rc1	No fix yet (0.8.0 unaffected)

References

- CVE-2013-2293
- Announcement (https://bitcointalk.org/?topic=144122)

- Gentoo bug (https://bugs.gentoo.org/show_bug.cgi?id=462046)

CVE-2013-3219

Date: 2013-03-11
Summary: Unenforced block protocol rule
Fix Deployment: 100%

Affected		Fix
Bitcoin-Qt bitcoind	0.8.0rc1 - 0.8.0	0.8.1

References

- BIP 50

CVE-2013-3220

Date: 2013-03-11
Summary: Inconsistent BDB lock limit interactions
Fix Deployment: 99.99%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.9rc1 0.5.0rc1 - 0.5.8rc1 0.6.0rc1 - 0.6.5rc1 0.7.0rc1 - 0.7.3rc1	0.4.9rc2 0.5.8rc2 0.6.5rc2 0.7.3rc2
wxBitcoin	ALL	NONE

References

- BIP 50

BIP-0034

Date: 2013-03-25
Summary: Mandatory block protocol update
Deployment: 100%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.7 0.5.0rc1 - 0.5.7 0.6.0rc1 - 0.6.0.9 0.6.1rc1 - 0.6.3	0.4.8rc1 0.5.7rc1 0.6.0.10rc1 0.6.4rc1
wxBitcoin	ALL	NONE

References

- BIP 0034

BIP-0050

Date: 2013-05-15
Summary: Hard fork to remove txid limit protocol rule
Deployment: 99.99%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.9rc1 0.5.0rc1 - 0.5.8rc1 0.6.0rc1 - 0.6.5rc1 0.7.0rc1 - 0.7.3rc1	0.4.9rc2 0.5.8rc2 0.6.5rc2 0.7.3rc2
wxBitcoin	ALL	NONE

References

- BIP 0050

CVE-2013-4627

Date: 2013-06-??
Summary: Memory exhaustion with excess tx message data
Fix Deployment: 99.9%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.9rc3 0.5.0rc1 - 0.5.8rc3 0.6.0rc1 - 0.6.5rc3 0.7.0rc1 - 0.7.3rc3 0.8.0rc1 - 0.8.3	0.4.9rc4 0.5.8rc4 0.6.5rc4 0.7.3rc4 0.8.4
wxBitcoin	ALL	NONE

References

CVE-2013-4165

Date: 2013-07-20
Summary: Timing leak in RPC authentication
Fix Deployment: 99.9%

Affected		Fix
Bitcoin-Qt bitcoind	* - 0.4.9rc3 0.5.0rc1 - 0.5.8rc3 0.6.0rc1 - 0.6.5rc3 0.7.0rc1 - 0.7.3rc3 0.8.0rc1 - 0.8.3	0.4.9rc4 0.5.8rc4 0.6.5rc4 0.7.3rc4 0.8.4rc1
wxBitcoin	ALL	NONE

References

- Bitcoin-Qt 0.8.4 release notes (https://bitcointalk.org/index.php?topic=287351)
- The initial bug report (https://github.com/bitcoin/bitcoin/issues/2838)

CVE-2013-5700

Date: 2013-09-04
Summary: Remote p2p crash via bloom filters
Fix Deployment: 99.9%

Affected		Fix
Bitcoin-Qt bitcoind	0.8.0rc1 - 0.8.3	0.8.4rc1

References

- Bitcoin-Qt 0.8.4 release notes (https://bitcointalk.org/index.php?topic=287351)
- The fix (https://github.com/bitcoin/bitcoin/commit/37c6389c5a0ca63ae3573440ecdfe95d28ad8f07)

- An added test (https://github.com/bitcoin/bitcoin/pull/18515)

CVE-2016-8889

Date: 2016-10-27
Summary: Debug console history storing sensitive info
Fix Deployment: 100%

Affected		Fix
Bitcoin Knots GUI	0.11.0 - 0.13.0	0.13.1

References

- Bitcoin Knots 0.16.1.knots20161027 release notes (https://github.com/bitcoinknots/bitcoin/blob/v0.13.1.knots20161027/doc/release-notes.md)
- US-CERT/NIST (https://nvd.nist.gov/vuln/detail/CVE-2016-8889)

CVE-2017-12842

Date: 2018-06-09
Summary: No commitment to block merkle tree depth

References

- Explanation by Sergio Demian Lerner (https://bitslog.wordpress.com/2018/06/09/leaf-node-weakness-in-bitcoin-merkle-tree-design/)
- Further elaboration by Suhas Daftuar (https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2019-February/016697.html)

CVE-2017-18350

Date: 2019-06-22
Summary: Buffer overflow from SOCKS proxy

Affected		Fix
Bitcoin-Qt bitcoind	0.7.0rc1 - 0.15.0	0.15.1rc1

References

- Disclosure of details (https://medium.com/@lukedashjr/cve-2017-18350-disclosure-fe6d695f45d5)

CVE-2018-17144

Date: 2018-09-17
Summary: Missing check for duplicate inputs
Fix Deployment: 31%

Affected		Fix
Bitcoin-Qt bitcoind	0.14.0rc1 - 0.14.2 0.15.0rc1 - 0.15.1 0.16.0rc1 - 0.16.2	0.14.3 0.15.2 0.16.3

References

- Full disclosure by Bitcoin Core (https://bitcoincore.org/en/2018/09/20/notice/)
- Bitcoin Core 0.16.3 release notes (https://bitcoincore.org/en/2018/09/18/release-0.16.3/)
- Bitcoin Knots 0.16.3.knots20180918 release notes (https://github.com/bitcoinknots/bitcoin/blob/v0.16.3.knots20180918/doc/release-notes.md)
- US-CERT/NIST (https://nvd.nist.gov/vuln/detail/CVE-2018-17144)
- Gentoo bug (https://bugs.gentoo.org/show_bug.cgi?id=666669)

CVE-2018-20586

Date: 2019-06-22
Summary: Debug log injection via unauthenticated RPC

Affected		Fix
Bitcoin-Qt bitcoind	0.12.0rc1 - 0.17.0	0.17.1rc1

CVE-2020-14199

Date: 2020-06-03
Summary: Double-signing can enable unintended fees

Affected		Fix
Trezor One		1.9.1
Trezor Model T		2.3.1
???		

References

- Disclosure of details by Trezor team (https://blog.trezor.io/details-of-firmware-updates-for-trezor-one-version-1-9-1-and-trezor-model-t-version-2-3-1-1eba8f60f2dd)

CVE-2020-26895

Date: 2020-10-08
Summary: Missing low-S normalization for HTLC signatures.

Affected		Fix
lnd		0.10.0

References

- CVE-2020-26895: LND Low-S Tx-Relay Standardness (https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002858.html)
- Full Disclosure: Full Disclosure: CVE-2020-26895 LND "Hodl my Shitsig" (https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002856.html)

CVE-2020-26896

Date: 2020-10-08
Summary: Invoice preimage extraction via forwarded HTLC.

Affected		Fix
lnd		0.11.0

References

- CVE-2020-26896: LND Invoice Preimage Extraction (https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002857.html)
- Full Disclosure: CVE-2020-26896 LND "The (un)covert channel" (https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002855.html)

CVE-2021-3401

Date: 2021-02-01

Summary: Qt5 remote execution

Affected		Fix
Bitcoin Core GUI		0.19.0
Bitcoin Knots GUI		0.18.1

CVE-2021-31876

Date: 2021-05-06

References

- Full Disclosure: CVE-2021-31876 Defect in Bitcoin Core's bip125 logic (https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2021-May/018893.html)

References

- URI Argument Injection Vulnerability in Bitcoin Core 0.18 and Earlier (https://achow101.com/2021/02/0.18-uri-vuln)

CVE-2023-50428

Date: 2023
Summary: Bypass of datacarriersize limit using OP_FALSE,OP_IF

Affected		Fix
Bitcoin Core	0.9 and later	NOT FIXED
Bitcoin Knots	0.9 - 23.0	25.1.knots20231115
btcd	?	NOT FIXED
libbitcoin	?	NOT FIXED

CVE-2024-34149

Date: 2024-03-30
Summary: Script size limit not enforced for Tapscript

Affected		Fix
Bitcoin Core	0.21.1 and later	NOT FIXED
Bitcoin Knots	0.21.1 - 23.0	25.1.knots20231115
btcd	?	?
libbitcoin	?	?

Definitions

A critical vulnerability is one that will have disastrous consequences if it is exploited. A serious vulnerability is one that will have serious consequences if it is exploited[1].

See Also

- Changelog
- https://blog.bitmex.com/bitcoins-consensus-forks/

References

1. http://bitcointalk.org/index.php?topic=88892.0 (http://bitcointalk.org/index.php?topic=88892.0)

Bitcoin Core documentation	
User documentation	Alert system • Bitcoin Core compatible devices • Data directory • Fallback Nodes • How to import private keys in Bitcoin Core 0.7+ • Installing Bitcoin Core • Running Bitcoin • Transaction fees • Vocabulary
Developer documentation	Accounts explained • API calls list • API reference (JSON-RPC) • Block chain download • Dump format • getblocktemplate • List of address prefixes • Protocol documentation • Script • Technical background of version 1 Bitcoin addresses • Testnet • Transaction Malleability • Wallet import format
History & theory	Common Vulnerabilities and Exposures • DOS/STONED incident • Economic majority • Full node • Original Bitcoin client • Value overflow incident