

# Common Vulnerabilities and Exposures

---

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

<a href="#">CVE-2012-2459</a>	2012-05-14	bitcoind and Bitcoin-Qt	Netsplit <sup>[1]</sup>	Easy	Block hash collision (via merkle root)	100% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-2459.html">http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-2459.html</a> )
<a href="#">CVE-2012-3789</a>	2012-06-20	bitcoind and Bitcoin-Qt	DoS <sup>[3]</sup>	Easy	(Lack of) orphan txn resource limits	100% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20123789">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20123789</a> )
<a href="#">CVE-2012-4682</a>		bitcoind and Bitcoin-Qt	DoS <sup>[3]</sup>			100% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-4682.html">http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-4682.html</a> )
<a href="#">CVE-2012-4683</a>	2012-08-23	bitcoind and Bitcoin-Qt	DoS <sup>[3]</sup>	Easy	Targeted DoS by CPU exhaustion using alerts	100% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-4683.html">http://luke.dashjr.org/programs/bitcoin/files/charts/CVE-2012-4683.html</a> )
<a href="#">CVE-2012-4684</a>	2012-08-24	bitcoind and Bitcoin-Qt	DoS <sup>[3]</sup>	Easy	Network-wide DoS using malleable signatures in alerts	100% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20124684">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20124684</a> )
<a href="#">CVE-2013-2272</a>	2013-01-11	bitcoind and Bitcoin-Qt	Exposure <sup>[6]</sup>	Easy	Remote discovery of node's wallet addresses	99.99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132272">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132272</a> )
<a href="#">CVE-2013-2273</a>	2013-01-30	bitcoind and Bitcoin-Qt	Exposure <sup>[6]</sup>	Easy	Predictable change output	99.99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132273">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132273</a> )

						<a href="http://org/programs/bitcoin/files/charts/security.html?20132273">org/programs/bitcoin/files/charts/security.html?20132273)</a>
<a href="#">CVE-2013-2292</a>	2013-01-30	bitcoind and Bitcoin-Qt	DoS <sup>[3]</sup>	Hard	A transaction that takes at least 3 minutes to verify	0% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132292">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132292)</a> )
<a href="#">CVE-2013-2293</a>	2013-02-14	bitcoind and Bitcoin-Qt	DoS <sup>[3]</sup>	Easy	Continuous hard disk seek	99.99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132293">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20132293)</a> )
<a href="#">CVE-2013-3219</a>	2013-03-11	bitcoind and Bitcoin-Qt 0.8.0	Fake Conf <sup>[8]</sup>	Miners <sup>[9]</sup>	Unenforced block protocol rule	100% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20133219">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20133219)</a> )
<a href="#">CVE-2013-3220</a>	2013-03-11	bitcoind and Bitcoin-Qt	Netsplit <sup>[1]</sup>	Hard	Inconsistent BDB lock limit interactions	99.99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20133220">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20133220)</a> )
<a href="#">BIP 0034</a>	2013-03-25	All Bitcoin clients	Fake Conf <sup>[8]</sup>	Miners <sup>[9]</sup>	Softfork: Height in coinbase	100% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/BIP-0034.html">http://luke.dashjr.org/programs/bitcoin/files/charts/BIP-0034.html</a> )
<a href="#">BIP 0050</a>	2013-05-15	All Bitcoin clients	Netsplit <sup>[1]</sup>	Implicit <sup>[2]</sup>	Hard fork to remove txid limit protocol rule	99.99% ( <a href="http://luke.dashjr.org/progr">http://luke.dashjr.org/progr</a>

						<a href="https://ams/bitcoin/files/charts/security.html?1750">ams/bitcoin/files/charts/security.html?1750)</a>
<a href="#">CVE-2013-4627</a>	2013-06-??	bitcoind and Bitcoin-Qt	DoS <sup>[3]</sup>	Easy	Memory exhaustion with excess tx message data	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20134627">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20134627)</a> )
<a href="#">CVE-2013-4165</a>	2013-07-20	bitcoind and Bitcoin-Qt	Theft <sup>[10]</sup>	Local	Timing leak in RPC authentication	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20134165">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20134165)</a> )
<a href="#">CVE-2013-5700</a>	2013-09-04	bitcoind and Bitcoin-Qt 0.8.x	DoS <sup>[3]</sup>	Easy	Remote p2p crash via bloom filters	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20135700">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20135700)</a> )
<a href="#">CVE-2014-0160</a>	2014-04-07	Anything using OpenSSL for TLS	Unknown <sup>[7]</sup>	Easy	Remote memory leak via payment protocol	Unknown
<a href="#">CVE-2015-3641</a> ( <a href="https://bitcoincore.org/en/2024/07/03/disclose_receive_buffer_oom/">https://bitcoincore.org/en/2024/07/03/disclose_receive_buffer_oom/</a> )	2014-07-07	bitcoind and Bitcoin-Qt prior to 0.10.2	DoS <sup>[3]</sup>	Easy	OOM via p2p	99.9% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20135700">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20135700)</a> )
BIP 66	2015-02-13	All Bitcoin clients	Fake Conf <sup>[8]</sup>	Miners <sup>[9]</sup>	Sofffork: Strict DER signatures	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?66">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?66)</a> )

BIP 65	2015-11-12	All Bitcoin clients	Fake Conf <sup>[8]</sup>	Miners <sup>[9]</sup>	Softfork: OP_CHECKLOCKTIMEVERIFY	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?65">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?65</a> )
BIPs 68, 112 & 113	2016-04-11	All Bitcoin clients	Fake Conf <sup>[8]</sup>	Miners <sup>[9]</sup>	Softforks: Rel locktime, CSV & MTP locktime	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?68">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?68</a> )
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 <sup>[8]</sup>	Miners <sup>[9]</sup>	Softfork: Segwit	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?141">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?141</a> )
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 <sup>[8]</sup>	Miners <sup>[9]</sup>	Softfork: Segwit UASF	?
CVE-2017-12842	2018-06-09				No commitment to block merkle tree depth	
CVE-2016-10724 ( <a href="https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-July/016189.html">https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-July/016189.html</a> )	2018-07-02	bitcoind and Bitcoin-Qt prior to 0.13.0	DoS <sup>[3]</sup>	Keyholders <sup>[11]</sup>	Alert memory exhaustion	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201610724">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201610724</a> )
TBD ( <a href="https://bitcoin">https://bitcoin</a> )	2024-07-03	Bitcoin Core/Knots	DoS <sup>[3]</sup>	Easy	OOM via fake block headers	

<a href="https://core.org/en/2024/07/03/disclose-header-spam/">core.org/en/2024/07/03/disclose-header-spam/</a>		prior to 0.15.0				
<a href="https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-July/016189.html">CVE-2016-10725 (https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-July/016189.html)</a>	2018-07-02	bitcoind and Bitcoin-Qt prior to 0.13.0	DoS <sup>[3]</sup>	Keyholders <sup>[11]</sup>	Final alert cancellation	99% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201610724">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201610724</a> )
<a href="#">CVE-2018-17144</a>	2018-09-17	bitcoind and Bitcoin-Qt prior to 0.16.3	Inflation <sup>[5]</sup>	Miners <sup>[9]</sup>	Missing check for duplicate inputs	80% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201817144">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201817144</a> )
<a href="https://medium.com/@lakedashjr/cve-2018-20587-advisory-and-full-disclosure-a3105551e78b">CVE-2018-20587 (https://medium.com/@lakedashjr/cve-2018-20587-advisory-and-full-disclosure-a3105551e78b)</a>	2019-02-08	Bitcoin Knots prior to 0.17.1, and all current Bitcoin Core releases	Theft <sup>[10]</sup>	Local	No alert for RPC service binding failure	<1% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201820587">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201820587</a> )
<a href="#">CVE-2017-18350</a>	2019-06-22	bitcoind and Bitcoin-Qt prior to 0.15.1	Unknown	Varies <sup>[12]</sup>	Buffer overflow from SOCKS proxy	94% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201718350">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201718350</a> )
<a href="#">CVE-2018-20586</a>	2019-06-22	bitcoind and Bitcoin-Qt prior to 0.17.1	Deception	RPC access	Debug log injection via unauthenticated RPC	77% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201820586">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201820586</a> )

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

<a href="https://en.bitcoin.it/wiki/2024/07/03/disclose-bip70-crash/">core.org/en/2024/07/03/disclose-bip70-crash/</a>		prior to 0.20.0				
<a href="https://cve.mitre.org/cve/2020/14199/">CVE-2020-14199</a>	2020-06-03	Trezor and others	Theft	Social <sup>[14]</sup>	Double-signing can enable unintended fees	
<a href="https://invdo.s.net/">CVE-2018-17145 (https://invdo.s.net/)</a>	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 <sup>[3]</sup>	Easy	p2p memory blow-up	87% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201817145">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?201817145</a> )
<a href="https://cve.mitre.org/cve/2020/26895/">CVE-2020-26895</a>	2020-10-08	Ind prior to 0.10	Theft	Easy	Missing low-S normalization for HTLC signatures	
<a href="https://cve.mitre.org/cve/2020/26896/">CVE-2020-26896</a>	2020-10-08	Ind prior to 0.11	Theft	Varies <sup>[15]</sup>	Invoice preimage extraction via forwarded HTLC	
<a href="https://bitcoincore.org/en/2024/07/03/disclose-unbounded-banlist/">CVE-2020-14198 (https://bitcoincore.org/en/2024/07/03/disclose-unbounded-banlist/)</a>		Bitcoin Core 0.20.1	DoS <sup>[3]</sup>	Easy	Remote DoS	93% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?202014198">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?202014198</a> )
<a href="https://bitcoincore.org/en/2024/07/03/disclose-timestamp-overflow/">TBD (https://bitcoincore.org/en/2024/07/03/disclose-timestamp-overflow/)</a>	2024-07-03	Bitcoin Core/Knots prior to 0.20.2	Netsplit <sup>[1]</sup>	Varies	Adjusted time manipulation	
<a href="https://cve.mitre.org/cve/2021/3401/">CVE-2021-3401</a>	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% ( <a href="http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20213401">http://luke.dashjr.org/programs/bitcoin/files/charts/security.html?20213401</a> )
<a href="https://bitcoincore.org/en/2024/07/31/disclose-oom-attack/">CVE-2024-52917 (https://bitcoincore.org/en/2024/07/31/disclose-oom-attack/)</a>	2024-07-31	Bitcoin Core/Knots prior to 22.0 with UPnP enabled	DoS	Local	OOM via LAN spam	

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

		0.21.1 - 0.23.0				
<a href="https://bitcoincore.org/en/2024/09/18/disclose-headers-oom/">CVE-2019-25220 (https://bitcoincore.org/en/2024/09/18/disclose-headers-oom/)</a>	2024-09-18	Bitcoin Core prior to 24.0.1 (Bitcoin Knots unaffected)	DoS <sup>[3]</sup>		Memory DoS due to headers spam	
<a href="https://bitcoincore.org/en/2024/10/08/disclose-mutated-blocks-hindering-propagation/">CVE-2024-52921 (https://bitcoincore.org/en/2024/10/08/disclose-mutated-blocks-hindering-propagation/)</a>	2024-10-09	Bitcoin Core/Knots prior to 25.0			Hindered block propagation due to mutated blocks	
<a href="https://bitcoincore.org/en/2024/10/08/disclose-large-inv-to-send/">TBD (https://bitcoincore.org/en/2024/10/08/disclose-large-inv-to-send/)</a>	2024-10-09	Bitcoin Core/Knots prior to 25.0			DoS due to inv-to-send sets growing too large	
<a href="https://bitcoincore.org/en/2024/10/08/disclose-blocktxn-crash/">CVE-2024-35202 (https://bitcoincore.org/en/2024/10/08/disclose-blocktxn-crash/)</a>	2024-10-09	Bitcoin Core/Knots prior to 25.0				
<a href="https://bitcoincore.org/en/2024/11/05/cb-stall-hindering-propagation/">CVE-2024-52922 (https://bitcoincore.org/en/2024/11/05/cb-stall-hindering-propagation/)</a>	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 \(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5137\)](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 \(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5141\)](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 \(http://blockexplorer.com/block/00000000000997f9fd2fe1ee376293ef8c42ad09193a5d2086dddf8e5c426b56\)](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 \(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5138\)](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 \(http://bitcointalk.org/index.php?topic=822.0\)](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=000000000790ab3, ver=1, hashPrevBlock=000000000606865, 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: 000000000790ab3f22ec756ad43b6ab569abf0bddeb97c67a6f7b1470a7ec1c

Transaction hash: 1d5e512a9723cbef373b970eb52f1e9598ad67e7408077a82fdac194b65333c9

## References

- [Discovery \(https://bitcointalk.org/index.php?topic=822.0\)](https://bitcointalk.org/index.php?topic=822.0)
- [US-CERT/NIST \(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5139\)](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 \(https://bitcointalk.org/index.php?topic=1306.0\)](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](https://en.bitcoin.it/wiki/BIP_0030))
- Gentoo bug tracker ([https://bugs.gentoo.org/show\\_bug.cgi?id=407793](https://bugs.gentoo.org/show_bug.cgi?id=407793))

- [US-CERT/NIST \(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1909\)](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
bitcoin for Windows	0.5.0rc1 - 0.5.0.4	0.5.0.5
Bitcoin-Qt for Windows	0.5.1rc1 - 0.5.3.0	0.5.3.1
	0.6.0rc1 - 0.6.0rc3	0.5.4
		0.6.0rc4

### References

- [Announcement \(https://bitcointalk.org/index.php?topic=69120.0\)](https://bitcointalk.org/index.php?topic=69120.0)
- [US-CERT/NIST \(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1910\)](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1910)
- [Full disclosure \(http://gavintech.blogspot.com/2012/03/full-disclosure-bitcoin-qt-on-windows.html\)](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	* - 0.4.4	0.4.5
bitcoin	0.5.0rc1 - 0.5.0.5	0.5.0.6
	0.5.1rc1 - 0.5.3	0.5.4rc1
	0.6.0rc1	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	0.4.6
	0.5.0rc1 - 0.5.5rc1	0.5.5
	0.6.0rc1 - 0.6.0.7rc1	0.6.0.7
	0.6.1rc1 - 0.6.1rc1	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 \(https://bitcointalk.org/?topic=81749\)](https://bitcointalk.org/?topic=81749)
- [Gentoo bug tracker \(https://bugs.gentoo.org/show\\_bug.cgi?id=415973\)](https://bugs.gentoo.org/show_bug.cgi?id=415973)
- [US-CERT/NIST \(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2459\)](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2459)
- [Full Disclosure \(https://bitcointalk.org/?topic=102395\)](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	0.4.7rc3
	0.5.0rc1 - 0.5.6rc2	0.5.6rc3
	0.6.0rc1 - 0.6.0.8rc2	0.6.0.9rc1
	0.6.1rc1 - 0.6.2.2	0.6.3rc1

## References

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

## CVE-2012-4682

---

**Date:**  
**Summary:**  
**Fix Deployment:** 100%

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

## References

- [CVE-2012-4682](#)
- [Gentoo bug \(https://bugs.gentoo.org/show\\_bug.cgi?id=435216\)](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	* - 0.4.7rc2	0.7.0
bitcoind	0.5.0rc1 - 0.5.6rc2	
	0.6.0rc1 - 0.6.0.8rc2	
	0.6.1rc1 - 0.6.2.2	

## References

- [CVE-2012-4683](#)
- [Announcement \(https://bitcointalk.org/index.php?topic=148038.0\)](https://bitcointalk.org/index.php?topic=148038.0)
- [Gentoo bug \(https://bugs.gentoo.org/show\\_bug.cgi?id=435216\)](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 \(https://bitcointalk.org/index.php?topic=148109.0\)](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 \(https://bitcointalk.org/?topic=135856\)](https://bitcointalk.org/?topic=135856)
- [Gentoo bug \(https://bugs.gentoo.org/show\\_bug.cgi?id=462046\)](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 \(https://bugs.gentoo.org/show\\_bug.cgi?id=462046\)](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 \(https://bitcointalk.org/?topic=140078\)](https://bitcointalk.org/?topic=140078)
- [Gentoo bug \(https://bugs.gentoo.org/show\\_bug.cgi?id=462046\)](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 \(https://bitcointalk.org/?topic=144122\)](https://bitcointalk.org/?topic=144122)

- [Gentoo bug \(https://bugs.gentoo.org/show\\_bug.cgi?id=462046\)](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	0.4.9rc2
	0.5.0rc1 - 0.5.8rc1	0.5.8rc2
	0.6.0rc1 - 0.6.5rc1	0.6.5rc2
	0.7.0rc1 - 0.7.3rc1	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 \(https://bitcointalk.org/index.php?topic=287351\)](https://bitcointalk.org/index.php?topic=287351)
- [The initial bug report \(https://github.com/bitcoin/bitcoin/issues/2838\)](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 \(https://bitcointalk.org/index.php?topic=287351\)](https://bitcointalk.org/index.php?topic=287351)
- [The fix \(https://github.com/bitcoin/bitcoin/commit/37c6389c5a0ca63ae3573440ecdfe95d28ad8f07\)](https://github.com/bitcoin/bitcoin/commit/37c6389c5a0ca63ae3573440ecdfe95d28ad8f07)

- [An added test \(https://github.com/bitcoin/bitcoin/pull/18515\)](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 \(https://github.com/bitcoinknots/bitcoin/blob/v0.13.1.knots20161027/doc/release-notes.md\)](https://github.com/bitcoinknots/bitcoin/blob/v0.13.1.knots20161027/doc/release-notes.md)
- [US-CERT/NIST \(https://nvd.nist.gov/vuln/detail/CVE-2016-8889\)](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 \(https://bitslog.wordpress.com/2018/06/09/leaf-node-weakness-in-bitcoin-merkle-tree-design/\)](https://bitslog.wordpress.com/2018/06/09/leaf-node-weakness-in-bitcoin-merkle-tree-design/)
- [Further elaboration by Suhas Daftuar \(https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2019-February/016697.html\)](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	0.14.3
	0.15.0rc1 - 0.15.1	0.15.2
	0.16.0rc1 - 0.16.2	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](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 \(https://blog.trezor.io/details-of-firmware-updates-for-trezor-one-version-1-9-1-and-trezor-model-t-version-2-3-1-1eba8f60f2dd\)](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 \(https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002858.html\)](https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002858.html)
- [Full Disclosure: Full Disclosure: CVE-2020-26895 LND "Hodl my Shitsig" \(https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002856.html\)](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 \(https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002857.html\)](https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002857.html)
- [Full Disclosure: CVE-2020-26896 LND "The \(un\)covert channel" \(https://lists.linuxfoundation.org/pipermail/lightning-dev/2020-October/002855.html\)](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<sup>[1]</sup>.

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

Retrieved from "[https://en.bitcoin.it/w/index.php?title=Common\\_Vulnerabilities\\_and\\_Exposures&oldid=70773](https://en.bitcoin.it/w/index.php?title=Common_Vulnerabilities_and_Exposures&oldid=70773)"

---

This page was last edited on 26 May 2025, at 16:22.

Content is available under [Creative Commons Attribution 3.0](#) unless otherwise noted.