PDF Export for report 1395694

Ongoing: Sentinel network proposal denial and bandwidth griefing

State	Informative
Reported by	Jacob Gadikian (jacobgadikian)
Reported to	Cosmos (cosmos)
Submitted at	2021-11-09T11:01:35.298Z (ISO-8601)
Asset	https://github.com/cometbft/cometbft (SOURCE_CODE)
References	
Weakness	
Severity	Medium (6.1) [CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H]
CVE IDs	

Summary:

- Since summer 2021, I have noticed extreme (100% of 1gbps) network utilization by sentinelhub on my relayer node\
- On October 29 or so, sentinelhub caused the OOM reaper to activate on my relayer node. This caused downtime across the cosmos IBC network and was widely reported.
- As I type this, my sentinel node is sending 36 Megabytes per second on a dedicated line that I have allocated to it. The blocks are empty.
- My Sentinelhub node is built with the exact code available at the sentinel repositories, except that it is using Tendermint 0.34.14 and that has been modified for debugging purposes
- Forbole was identified as the signer of malicious blocks with 336 blockparts, which occured routinely and caused bandwidth usage to spike to tens of megabytes per second. Forbole states that they were running an unmodified binary and had incorrectly set the minimum gas fee. Notional efforts to replicate this resolution with a changed gas fee have not been successful.

In order to get here I:
- Spent 10 days of my personal time and 10 days of my team's time
- Custom built a computer to dedicate to debugging
- Dedicated a 500mbps fiber optic line to Sentinel
- Moved my Sentinel validator between four machines on two continents
- Deferred other work tasks for myself and my consultancy, Notional

Steps To Reproduce:

[add details for how we can reproduce the issue]
1. Connect to the sentinel network
2. Wait
    1. Observe invald blocks containing 336 blockparts each.
    2. Observe bandwidth usage. For example, my node has been up about 2 hours and has used 200GB of bandwidth. Gigabytes.

The following nodes were identified as suspect, but the attacker (?!) knows how to replicate and it's a game of whack a mole.

updated list of asshole nodes

159.203.174.29
3.239.11.246
54.169.185.248
142.93.72.221
13.212.44.171
13.212.44.172
135.181.16.236
144.76.154.125
35.215.62.70
65.21.129.165
35.163.249.152
68.183.119.113
88.198.129.19
104.198.198.7

Example of attacker using programmatically generated monikers:

"id": "baed7d33417bb82cdaab2d046138c1d82be9bc53",
"listen_addr": "tcp://51.222.40.130:26656",
"network": "sentinelhub-2",
"version": "v0.34.12",
"channels": "40202122233038606100",
"moniker": "crfbBJohWr",
"other": {
"tx_index": "on",
"rpc_address": "tcp://0.0.0.0:26657"
}

Numerals are bytes:
7012734191 410873887 baed7d33417bb82cdaab2d046138c1d82be9bc53@51.222.40.130:26656 crfbBJohWr
5059630354 323541775 09532f888c0fd9358826d68761c20c2853f90169@165.227.34.33:26656 oixBU9qxdn
663779330 11611166622 059749e2ddfb9755e160617159e3cd0d0e8871c4@35.230.37.28:26656 archive

Supporting Material/References:

Yeah, here's an 8gb log file of the debug log, you can retrieve using IPFS

http://ipfs.io/ipfs/QmQKPwQsD9znteGDtQSuKDxjHpJUDJzvJtQtJCJ49YZDTu

I've kept records of the telegram chat this has been discussed in, too, because some highly unlikely statements have been made. Contact me for this or for contextual information, your choice.

2:15PM INF received proposal module=consensus proposal={"Type":32,"block_id":{"hash":"9C86609F7297F33214D777CC6EBE7C8B2B3780349546818565F281363D5E20E2","parts":{"hash":"CED9CB6C468F54D8EB0DA600038E1EE029D73F04290B4B173964C0EA56CA6CF9","total":336}1,"round":0,"signature":"9LeyIuxfyTQV0yRoULkTpwTDh+WkO/e5Y7j7mivU1mH+Qz1CB7VlaXXUBLS4TPz11-09T07:15:03.029015254Z"}

height 3207860
round 0
proposer 7A6A3EB9A5DED56929E2E9465CB48D5A553D8578

208044818

height 3207860
round 0
proposer 7A6A3EB9A5DED56929E2E9465CB48D5A553D8578

208044818

2:15PM INF Timed out dur=2000 height=3207860 module=consensus round=0 step=7

height 3207860
round 1
proposer CD95831EE1DC61F728D569545DA4CC5593563D38

208044818

height 3207860
round 1
proposer CD95831EE1DC61F728D569545DA4CC5593563D38

208044818

height 3207860
round 1
proposer CD95831EE1DC61F728D569545DA4CC5593563D38

208044818

==========
height 3201052
round 0
proposer F9879C1198FA5704046638B2DF4518B08981F573
2:02AM INF received proposal module=consensus proposal={"Type":32,"block_id":{"hash":"D52235D324A69A4B6749986202BB521440F9FC77C63060B7BEF740DF60E8DC27","parts":{"hash":"59F8B26FC1C011A3891C0A3F7C4C4EE70ABFED6CD4DB8ED086472AE2E981EF22","total":336}},"height":3201052,"pol_round":-1,"round":0,"signature":"+pLlgcc/zQnjmjBp5TZr+fVrjb7X9UnanCcpMZQ11LPc713g8s1LVzt1vMuxR8G14JaHQXNADvmTQGLL926bDQ==","timestamp":"2021-11-08T19:02:15.480217789Z"}

2:02AM INF Timed out dur=3000 height=3201052 module=consensus round=0 step=3

height 3201052
round 0
proposer F9879C1198FA5704046638B2DF4518B08981F573

2:02AM INF Timed out dur=1000 height=3201052 module=consensus round=0 step=7

height 3201052
round 1
proposer B0A775D0DEA4C1D6CFA7A9543C351428E70778C3
2:02AM INF commit is for a block we do not know about; set ProposalBlock=nil commit=FF37A8A01320A1A81B79270BF35FA5131B9B75D5C9A53217EEE3FDBB876B5690 commit_round=1 height=3201052 module=consensus proposal=
2:02AM INF Timed out dur=3500 height=3201052 module=consensus round=1 step=3
2:02AM INF Saving AddrBook to file book=sentry/config/addrbook.json module=p2p size=202
2:02AM INF Ensure peers module=pex numDialing=0 numInPeers=0 numOutPeers=7 numToDial=93
2:02AM INF Will dial address addr={"id":"540607e0df279dd29a62330dbbab2bf25213f00e","ip":"52.207.8.63","port":26656} module=pex
2:02AM INF Will dial address addr={"id":"a59c11059bcf9bc5fd7014a7462d4efb55e2e888","ip":"144.76.219.156","port":18856} module=pex
2:02AM INF Will dial address addr={"id":"e79ece514fd515491f536d7a478aedde0767585e","ip":"34.211.185.245","port":26656} module=pex
2:02AM INF Will dial address addr={"id":"07c20b96c6497b1b01af1713a9c834c239df7278","ip":"51.75.52.109","port":23656} module=pex
2:02AM INF Will dial address addr={"id":"a93eb2df1ec486d12246e690e3ef466dcfb26394","ip":"46.101.184.221","port":26656} module=pex
2:02AM INF Will dial address addr={"id":"90671c1fcce87548a8326168bb6ae01f9d642ac5","ip":"18.202.106.77","port":26656} module=pex
2:02AM INF Will dial address addr={"id":"9f5d816ffdd920ecaca60cfc575e730a1f827038","ip":"162.251.237.61","port":26656} module=pex
2:02AM INF Will dial address addr={"id":"6a124b82d92b6c2b34e87004fc60ae15e4a1d8be","ip":"34.192.217.139","port":26656} module=pex
2:02AM INF Will dial address addr={"id":"34a54286894e4073def7bf3bc14d21db0fd949af","ip":"18.144.134.123","port":26656} module=pex
2:02AM INF Will dial address addr={"id":"fbbfcb3203bf401c8aff274c5f78870329bd41c5","ip":"52.60.52.207","port":26711} module=pex

Impact

Net Effect

- I'm not relaying sentinel anymore
- The sentinel network is very difficult to achieve connections on
- Sentinel Validators are being griefed to death
- I believe there's a consensus issue that causes p2p to gossip block proposals regardless of validity and that this can be used to be used to deny block proposals. It is uncertain at this time if this is targeted, though evidence suggests that it may be.

Activity

Hey @jacobgadikian
Thanks for taking time to submit this report to our bug bounty program. I can't map the context to a scoped issue so I'm going to close this report as informative.

mizmo	2023-08-08 19:05	bug informative	Public

curl 'https://rpc-osmosis-archive-yxeh2xenrmfragql-ie.internalendpoints.notional.ventures/tx_search?query=%22send_packet.packet_src_channel=%27channel-0%27%20AND%20send_packet.packet_sequence=%271275507%27%22%E2%80%99

Jacob Gadikian	2023-01-10 10:41	comment	Public

thanks man. FYI, working with ibc team on something that could be related to this at present

Jacob Gadikian	2023-01-10 10:38	comment	Public

Thanks Jacob, we're still investigating how best to handle this. Did Khanh make another report on HackerOne or its somewhere else?

Ethan Buchman	2021-12-03 05:13	comment	Public

So, as I mentioned on twitter, after I made this report, Khanh Nguyen made a second report after mine. It is more detailed and includes code to monitor the attack live.

It is also very reasonalbe to assume that Gaia could be attacked this way but they don't make Winnie the Pooh memes mocking Xi Jinping, so wasn't targeted.

Jacob Gadikian	2021-11-27 15:16	comment	Public

I think that "stop peers due to bad proposals" would maybe help. Thing is, We got the feeling that all of this was being done from some random RPC.

Only way to know for sure would be to wrap the sentinel valset in a VPN. By doing this we could know for sure. Of course you're right about the difficulties of debugging a live network.

Jacob Gadikian	2021-11-27 15:14	comment	Public

Sure, we went from ahole nodes to evil nodes then to indicator nodes.

I am reading through the issue mentioned now.

Khanh has also made a second report.

336 is the maximum number of blockparts.

Jacob Gadikian	2021-11-27 15:11	comment	Public

Hi Jacob, thanks for the report, and for your patience.

It's a bit difficult to reproduce reports that require connecting to a live network. Can you try to give some more clarity on whats happening here? Are you suggesting that a malicious block proposer can send large invalid blocks to mess with the consensus? Or that some other node can send faulty proposals? Presumably these blocks never actually get committed ? It's hard to see whats going on from the logs you've sent - maybe you could provide another snippet that shows clearly what is happening (8gb is surely too much for us to work through)? Also do you know if there is something significant about that 336 number?

At some level, it's already a known issue that Tendermint needs more defences in the consensus reactor:https://github.com/tendermint/tendermint/issues/2871. Do you think this report falls into something there or you think it's somehow different?
updated list of asshole nodes
We would ask that you refrain from using this kind of language, please and thank you!

Ethan Buchman	2021-11-27 14:31	comment	Public

Hi, this is still occuring, and I'm strongly considering disclosing as an issue on tm/sdk repos.

Jacob Gadikian	2021-11-26 18:46	comment	Public

yes, my report can be reproduced and the steps are to join the sentinel network.

Impact: somehow I reckon this could be used to kill chains.

Yeah, it's in scope. This is ongoing, and I'll be updating the report.

Jacob Gadikian	2021-11-09 11:03	comment	Public