Hello All!

I have chosen CVE-2018-17145 the “Bitcoin Inventory Out-of-Memory Denial-of-Service Attack”

This was a vulnerability that effected Bitcoin core users prior to the 0.16.2 version and all other forks based off that code base. At a high level this vulnerability was a Denial-of-Service attack based off uncontrolled resource consumption. The Bitcoin protocol uses many messaging types and the one used to exploit in this attack is the inventory (Inv) message type. The Inv, allows a node to advertise it knowledge of one or more objects. Before the update preventing this, a hostile node could cause a DOS to a neighboring peer by flooding it with Inv messages with faulty transactions and hashes. This caused the victims memory to be used up until it crashed, or the process was terminated. It has been argued that this vulnerability didn’t necessarily put your blockchain assets at risk but could freeze your node if you were running one. Theoretically on a large scale this could of been implemented to knock out other competing nodes on the network, decreasing competition. To protect yourself from this vulnerability, make sure to be running Bitcoin Core 0.16.2 or greater. I find this interesting because in the day and age of digital assets its important that these code bases are revised for a greater security posture, and this a great example of that.

Thanks again!

-ERIC WEBB

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17145