

Forum:[Hack Forums](#)

Thread: [Bitcoin wallet.dat extraction from bitcoin binary crash dumps](#)

oxagast - March 3, 2022, 6:18 am

My write-up on how CVE-2019-15947 works; a way to extract bitcoin wallet.dat files from crash dumps. Working on a way to extract the encrypted wallet.dat from bitcoin-qt crash dumps, but that is going to be quite a bit more involved. The private key is stored in memory so bitcoin-qt itself can read the plaintext wallet, so it should be possible. This code however is designed to work on unencrypted wallets.

The writeup: <https://oxagast.org/posts/CVE-2019-15947-bitcoin-wallet-dat-core-dumps-design-flaw/>

Here is the GitHub issue thread on the vulnerability: <https://github.com/bitcoin/bitcoin/issues/16824>

The full exploit:

<https://github.com/oxagast/oxasploits/blob/master/exploits/CVE-2019-15947/makeittrain.sh>

Thanks, and let me know how you like it!

oxagast

Abraham - June 20, 2022, 1:51 pm

This is really great work, good job on this exploit.

_daniel - June 20, 2022, 8:25 pm

Nice work. I noticed you shared in your blog post that you work a day job in fast food. Why don't you try this across different blockchain projects bug-bounty programs? I'm sure other software implementations would be vulnerable to similar exploits, and a lot of these projects pay big for responsible disclosure.

rabbi - June 20, 2022, 8:35 pm

Great write up. Consider hosting your site for free with GitHub Pages.