**Bug description:**

RpcDSSMoveFromSharedFile(handle,L"token",L"c:\\blah1\\pci.sys");

This function exposed over alpc, has a arbitrary delete vuln.

Hitting the timing was pretty annoying. But my PoC will keep rerunning until c:\windows\system32\drivers\pci.sys is deleted.

I believe it’s impossible to hit the timing on a single core VM. I was able to trigger it using 4 cores on my VM. (Sadly I wasn’t able to use OPLOCKS with this particular bug)

Root cause is basically just a delete without impersonation because of an early revert to self. Should be straight forward to fix it…

Exploitation wise.. you either try to trigger dll hijacking issues in 3rd party software.. or delete temp files used by a system service in c:\windows\temp and hijack them and hopefully do some evil stuff.