VMware ThinApp DLL hijacking vulnerability

From: houjingyi <houjingyi647 () gmail com>
Date: Wed, 14 Jul 2021 11:35:13 +0800

A few months ago I disclosed IBM(R) Db2(R) Windows client DLL Hijacking Vulnerability(0day) I found:

https://seclists.org/fulldisclosure/2021/Feb/73

In that post I mentioned the vulnerability did not get fully patched.

After I told IBM on hackerone that I disclosed it, hackerone asked me to delete the post, IBM apologized and fully patched the vulnerability.

But this is not the point today. I found a similar problem in VMware-ThinApp-Enterprise-5.2.9-17340778.exe.

After install the software create C:\DummyTLS and rename a dll you want to load to dummyTLS.dll and put it to C:\DummyTLS\dummyTLS.dll.

Run "C:\Program Files (x86)\VMware\VMware ThinApp\Setup Capture.exe" and C:\DummyTLS\dummyTLS.dll will be loaded.
(other exe like log_monitor.exe/snapshot.exe vulnerable too).

This is also because they use code like:

```
LoadLibraryExW(L"\\DummyTLS\\dummyTLS.dll", 0, 0);
```

In short, Windows will treat relative path in LoadLibrary(and many other functions) as the path rooted relative to the current disk designator.

Let us look into code in ntdll.dll. The logic here is:
KernelBase!LoadLibraryExW->ntdll!LdrpLoadDll->ntdll!LdrpPreprocessDllName.
In LdrpPreprocessDllName after calling RtlDetermineDosPathNameType_Ustr it will return 4(RtlPathTypeRooted).

And after calling LdrpGetFullPath we get "C:\DummyTLS\dummyTLS.dll"!

You should not call LoadLibrary with the relative path. In fact, using relative path is dangerous in many cases.

This was fixed in 2021-07-13 as CVE-2021-22000 and the advisory is here : https://www.vmware.com/security/advisories/VMSA-2021-0015.html.

For these vulnerabilities I will post a summary at https://houjingyi233.com.

____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

Current thread:

VMware ThinApp DLL hijacking vulnerability ***houjingyi (Jul 16)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License