VMware ThinApp DLL Hijacking

Authored by houjingyi

Posted Jul 16, 2021

VMware ThinApp suffered from a dll hijacking vulnerability.

tags | exploit
systems | windows
advisories | CVE-2021-22000
SHA-256 | dedc1cfb4f333940026e5b2b4d856aefcdc832256f158ccb6dd78653a41dfcfb

Download | Favorite | View

Related Files

Share This

Change Mirror Download

```
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.
```

Login or Register to add favorites

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

- Red Hat 180 files
- Ubuntu 78 files
- Debian 24 files
- LiquidWorm 23 files
- malvuln 12 files
- nu11secur1ty 10 files
- Gentoo 9 files
- Google Security Research 8 files
- T. Weber 4 files
- Julien Ahrens 4 files

File Tags

- ActiveX (932)
- Advisory (79,733)
- Arbitrary (15,694)
- BBS (2,859)
- Bypass (1,619)
- CGI (1,018)
- Code Execution (6,924)
- Conference (673)
- Cracker (840)
- CSRF (3,290)
- DoS (22,601)
- Encryption (2,349)
- Exploit (50,358)
- File Inclusion (4,165)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,660)
- Intrusion Detection (867)
- Java (2,899)
- JavaScript (820)
- Kernel (6,290)
- Local (14,201)
- Magazine (586)
- Overflow (12,418)
- Perl (1,418)
- PHP (5,093)
- Proof of Concept (2,291)
- Protocol (3,435)
- Python (1,467)
- Remote (30,043)
- Root (3,504)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,776)
- Shell (3,103)
- Shellcode (1,204)
- Sniffer (886)

File Archives

- December 2022
- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- Older

Systems

- AIX (426)
- Apple (1,926)
- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,634)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,294)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,448)
- Slackware (941)
- Solaris (1,607)

Spoof (2,166)
SQL Injection (16,101)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,132)
Web (9,357)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,158)
UnixWare (185)
Windows (6,511)
Other

packet storm

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed