59 Arbitrary code execution in desktop client via OpenSSL config

Share:

TIMELINE

0ph0le submitted a report to Nextcloud. Jun 20th (3 years ago)

Summary:
The nextcloud windows desktop application utilizes a precompiled OpenSSL library called libeay32.dll. This OpenSSL library attempts to load c:\usr\local\ssl\openssl.cnf when the nextcloud windows application is launched. The c:\usr\local\ssl\openssl.cnf file does not exist. By default, on windows systems, authenticated users can create under the c: drive. A user with low privileges can create the file c:\usr\local\ssl\openssl.cnf configuration file to load a nefarious .dll library, resulting in arbitrary code execution when the nextcloud windows application is launched (by any user including an administrator).

Description:
If you download sys internals process monitor, you can see the "nextcloud.exe" binary trying to read the files "c:\usr\local\ssl\openssl.cnf" and getting a result of "PATH NOT FOUND". See attached openssl-not-found.png screenshot.

The root cause of the issue is when the OpenSSL library (libeay32.dll) was compiled, the parameter "--openssldir" was not specified. If this parameter is not specified, a default of "/usr/local/ssl" is used. This is a real directory in linux, but in windows it translates to c:\usr\local\ssl.

If a low privilege user creates the directory structure c:\usr\local\ssl\, copies an openssl.cnf file and malicious .dll library inside it will result is arbitrary code execution when the nextcloud application is executed. If the nextcloud application is executed by an administrator, it will result in privilege escalation.

I've included two example exploits;

Exploit example 1
calc.c – source code of my .dll file to execute calc.exe
calc.dll – compiled version of the calc.exe library
openssl-calc.cnf – openssl configuration file that calls the calc.dll

Exploit example 2
backdoor.c – source code my .dll file to create a local administrator, this uses a known uac bypass
backdoor.dll – compiled version of the local admin backdoor library
openssl-backdoor.cnf – openssl configuration file that calls the backdoor.dll

Platform(s) Affected:
All supported windows platforms that support Nextcloud Desktop 2.5.2

Steps To Reproduce:
Download and Install Nextcloud desktop 2.5.2 (https://nextcloud.com/install/#install-clients)

Exploit 1 – calc.exe – See attached video calc.mp4

1. Login with a low privileged user (part of Users group)
2. Open a cmd.exe and issue command: mkdir c:\usr\local\ssl
3. Copy calc.dll and openssl-calc.cnf to c:\usr\local\ssl directory
4. Rename c:\usr\local\ssl\openssl-calc.cnf to c:\usr\local\ssl\openssl.cnf
5. Logout of low privledged user.
6. Login with local administrator.
7. Launch Nextcloud application.
8. Calc.exe with execute.

Exploit 2 – create a local admin user (uac bypass) – See attached video backdoor.mp4

1. Login with a low privileged user (part of Users group)
2. Open a cmd.exe and issue command: mkdir c:\usr\local\ssl
3. Copy calc.dll and openssl-backdoor.cnf to c:\usr\local\ssl directory
4. Rename c:\usr\local\ssl\openssl-backdoor.cnf to c:\usr\local\ssl\openssl.cnf
5. Logout of low privledged user.
6. Login with local administrator.
7. Launch Nextcloud application.
8. Open "Computer Management"
9. Navigate to "System Tools" -> "Local Users and Groups" -> "Users"
10. A new user of "backdoor" with a password of "backdoor" was added.
11. Right click on "backdoor" and click "Properties", then click "Member Of".
12. The "backdoor" user is part of the local administrator group.

Supporting Material/References:
https://wiki.openssl.org/index.php/Compilation_and_Installation#PREFIX_and_OPENSSLDIR

How can the system be exploited with this bug?
DLL Hi-jacking can be used for many nefarious purposes. It can be used by malware to propagate and establish persistence on a workstation. It can be used to privilege escalation in the post exploitation phases of an attack.

How did you come across this bug ?
I can across this while looking for programs that utilize the windows openssl (libeay32.dll) library.
Recommendations for fix
Recompile the openssl library (libeay32.dll), and specify the parameter "—openssldir". Set the directory to something a low privledge user can't edit for example "C:\Program Files (x86)\Nextcloud". Use the link in the support material / references part of this report.

Impact

9 attachments:
F513310: backdoor-uac.c
F513311: backdoor-uac.dll
F513312: calc.c
F513313: calc.dll
F513314: backdoor.mp4
F513315: openssl-backdoor.cnf
F513316: openssl-calc.cnf
F513317: calc.mp4
F513318: openssl-not-found.png