



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

Shrew Soft VPN Client 2.2.2 - 'iked' Unquoted Service Path

EDB-ID:

47660

CVE:

N/A

EDB Verified: ✘

Author:

[D.GOEDECKE](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2019-11-15

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Shrew Soft VPN Client 2.2.2 - 'iked' Unquoted Service Path
# Date: 2019-11-14
# Exploit Author: D.Goedecke
# Vendor Homepage: www.shrew.net
# Software Link: https://www.shrew.net/download/vpn/vpn-client-2.2.2-
release.exe
# Version: 2.2.2
# Tested on: Windows 10 64bit
```

```
C:\Users\user>wmic service get name, displayname, pathname, startmode |
findstr /i "auto" | findstr /i /v "C:\Windows\\" | findstr /i /v ""
ShrewSoft IKE Daemon iked C:\Program
Files\ShrewSoft\VPN Client\iked.exe -service Auto
ShrewSoft IPSEC Daemon ipsecd C:\Program
Files\ShrewSoft\VPN Client\ipsecd.exe -service Auto
```

```
C:\Users\user>sc qc iked
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: iked
        TYPE                : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program Files\ShrewSoft\VPN Client\iked.exe
        -service
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME         : ShrewSoft IKE Daemon
        DEPENDENCIES         :
        SERVICE_START_NAME  : LocalSystem
```

```
C:\Users\user>sc qc ipsecd
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: ipsecd
        TYPE                : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program Files\ShrewSoft\VPN
Client\ipsecd.exe -service
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME         : ShrewSoft IPSEC Daemon
        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](#)



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

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