

 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

Hotspot Shield 6.0.3 - Unquoted Service Path Privilege Escalation

EDB-ID:

40528

CVE:

N/A

EDB Verified: 

Author:

[AMIR.GHT](#)

Type:

[LOCAL](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2016-10-13

Vulnerable App: 



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

```
#####
# Exploit Title: Hotspot Shield Unquoted Service Path Privilege Escalation
# Date: 13/10/2016
# Author: Amir.ght
# Vendor Homepage: https://www.hotspotshield.com
# Software Link: https://www.hotspotshield.com/download/
# version : 6.0.3 (Latest)
# Tested on: Windows 7
#####
```

Hotspot Shield installs as 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 hshld
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: hshld
        TYPE                : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program Files\Hotspot
Shield\bin\cmw_srv.exe
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME        : Hotspot Shield Service
        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.