

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



**Cookiebot**  
by Usercentrics

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

# Hotspot Shield 6.0.3 - Unquoted Service Path Privilege Escalation

**EDB-ID:**

40528

**CVE:**

N/A

**EDB Verified:** ✓

**Author:**

[AMIR.GHT](#)

**Type:**

[LOCAL](#)

**Exploit:** /



**Cookiebot**  
by Usercentrics

### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

```
#####
# 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
```



Cookiebot  
by Usercentrics

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC TERMS PRIVACY ABOUT US FAQ COOKIES

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