IObit Advanced SystemCare 10.0.2 - Unquoted Service Path Privilege Escalation

EDB-ID:
40577

CVE:
N/A

EDB Verified: ✓

Author:
AMIR.GHT

Type:
LOCAL

Exploit: / {}

```
##############################################################################
# Exploit Title: IObit Advanced SystemCare Unquoted Service Path Privilege
Escalation
# Date: 19/10/2016
# Author: Ashiyane Digital Security Team
# Vendor Homepage: http://www.iobit.com/en/index.php
# Software Link: http://www.iobit.com/en/advancedsystemcarefree.php#
# version : 10.0.2  (Latest)
# Tested on: Windows 7
##############################################################################

IObit Advanced SystemCare 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 AdvancedSystemCareService10
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: AdvancedSystemCareService10
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
```