



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

IObit Malware Fighter 4.3.1 - Unquoted Service Path Privilege Escalation

EDB-ID:

40525

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



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
#####
# Exploit Title: IObit Malware Fighter Unquoted Service Path Privilege
Escalation
# Date: 12/10/2016
# Author: Amir.ght
# Vendor Homepage: http://www.iobit.com/en/index.php
# Software Link:
http://www.iobit.com/downloadcenter.php?product=malware-fighter-free
#version : 4.3.1 (Latest)
# Tested on: Windows 7
#####
```

IObit Malware Fighter installs two 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 IMFservice
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: IMFservice
        TYPE                : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program Files\IObit\IObit Malware
Fighter\IMFsrv.exe
        LOAD_ORDER_GROUP    : System Reserved
        TAG                  : 1
        DISPLAY_NAME         : IMF Service
        DEPENDENCIES         :
        SERVICE_START_NAME  : LocalSystem
```

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

```
SERVICE_NAME: LiveUpdateSvc
        TYPE                : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program
Files\IObit\LiveUpdate\LiveUpdate.exe
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME         : LiveUpdate
        DEPENDENCIES         :
        SERVICE_START_NAME  : LocalSystem
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

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

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING