

 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

NETGATE Registry Cleaner 16.0.205 - Unquoted Service Path Privilege Escalation

EDB-ID:

40539

CVE:

N/A

EDB Verified: 

Author:

[AMIR.GHT](#)

Type:

[LOCAL](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2016-10-15

Vulnerable App: 



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

```
#####
# Exploit Title: NETGATE Registry Cleaner Unquoted Service Path Privilege Escalation
# Date: 15/10/2016
# Author: Amir.ght
# Vendor Homepage: http://www.netgate.sk/
# Software Link: http://www.netgate.sk/download/download.php?id=4
# Version : build 16.0.205 (Latest)
# Tested on: Windows 7
#####
```

NETGATE Registry Cleaner 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 NGRegClnSrv
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: NGRegClnSrv
        TYPE                : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2   AUTO_START
        ERROR_CONTROL        : 1   NORMAL
        BINARY_PATH_NAME     : C:\Program Files\NETGATE\Registry
Cleaner\RegistryCleanerSrv.exe
        LOAD_ORDER_GROUP    :
        TAG                  : 0
        DISPLAY_NAME        : NETGATE Registry Cleaner Service
        DEPENDENCIES        :
        SERVICE_START_NAME  : LocalSystem
```

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

OffSec Services Limited 2026. All rights reserved.