Cyber Solutions

Product Security Advisory

July 18, 2019

JCI-PSA-2019-03 v2
CVE-2019-7590

Affected Product

Johnson Controls Cyber Solutions has confirmed a vulnerability in certain versions of the exacqVision Server application. In the affected versions, an attacker could obtain privilege escalation without authorization. This advisory provides guidance on mitigation actions to avoid a potential exploit.

Overview

This vulnerability only impacts exacqVision Server 9.6 and 9.8 running on a Windows operating system (all supported versions of Windows). This issue does not impact Linux deployments with permissions that are not inherited from the root directory.

Mitigation

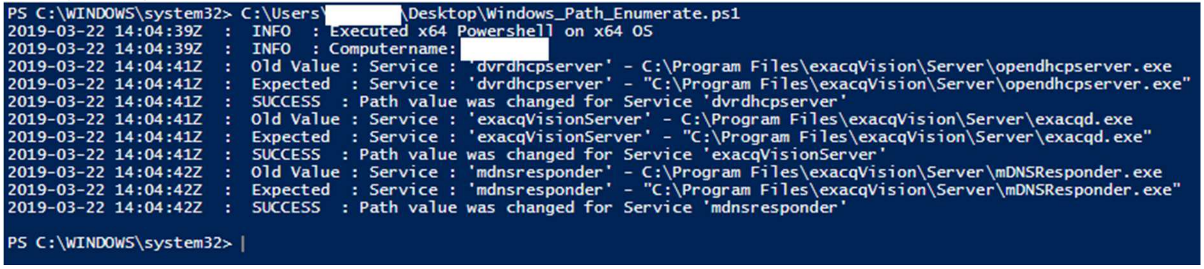
This issue is resolved in exacqVision Server 19.03, which was released on March 15, 2019. While this fix is currently available, it is also possible to patch exacqVision versions 9.6 or 9.8 running on Windows operating systems as a temporary action. The patch addresses the vulnerability and can be applied via script (option 1) or through a manual action (option 2). To leverage the full benefit of the newer release, Johnson Controls Cyber Solutions recommends upgrading patched systems to version 19.03.

Option 1 (script applied patch)

1. Download the PowerShell script found here: https://gallery.technet.microsoft.com/scriptcenter/Windows-Unquoted-Service-190f0341 or https://github.com/VectorBCO/windows-path-enumerate

2. Open an escalated PowerShell window and run the script.

Example output:



```
PS C:\WINDOWS\system32> C:\Users\[redacted]\Desktop\Windows_Path_Enumerate.ps1
2019-03-22 14:04:39Z  :  INFO   : Executed x64 Powershell on x64 OS
2019-03-22 14:04:39Z  :  INFO   : Computername: [redacted]
2019-03-22 14:04:41Z  :  Old Value : Service : 'dvrdhcpserver' - C:\Program Files\exacqVision\Server\opendhcpserver.exe
2019-03-22 14:04:41Z  :  Expected  : Service : 'dvrdhcpserver' - "C:\Program Files\exacqVision\Server\opendhcpserver.exe"
2019-03-22 14:04:41Z  :  SUCCESS  : Path value was changed for Service 'dvrdhcpserver'
2019-03-22 14:04:41Z  :  Old Value : Service : 'exacqVisionServer' - C:\Program Files\exacqVision\Server\exacqd.exe
2019-03-22 14:04:41Z  :  Expected  : Service : 'exacqVisionServer' - "C:\Program Files\exacqVision\Server\exacqd.exe"
2019-03-22 14:04:41Z  :  SUCCESS  : Path value was changed for Service 'exacqVisionServer'
2019-03-22 14:04:42Z  :  Old Value : Service : 'mdnsresponder' - C:\Program Files\exacqVision\Server\mDNSResponder.exe
2019-03-22 14:04:42Z  :  Expected  : Service : 'mdnsresponder' - "C:\Program Files\exacqVision\Server\mDNSResponder.exe"
2019-03-22 14:04:42Z  :  SUCCESS  : Path value was changed for Service 'mdnsresponder'

PS C:\WINDOWS\system32> |
```

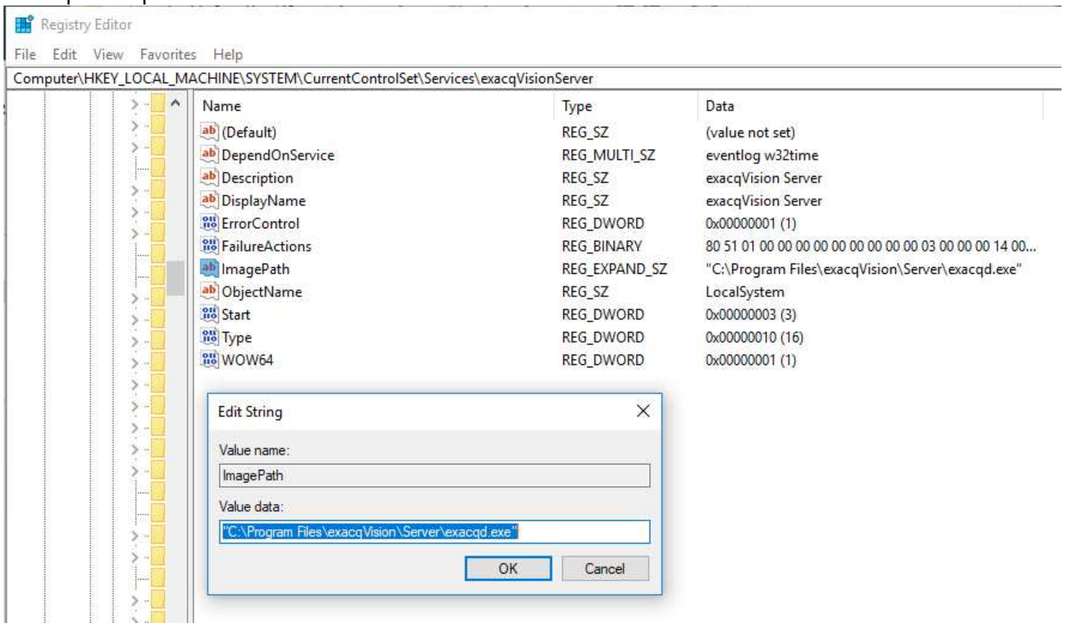
Option 2 (manually applied patch)

1. Run Registry Editor and navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\exacqVisionServer.

2. Modify the ImagePath for to include quotations around the entire file path.

3. Repeat this process for HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dvrdhcpserver and HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mdnsresponder

Example output:



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\exacqVisionServer

Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_MULTI_SZ	eventlog w32time
Description	REG_SZ	exacqVision Server
DisplayName	REG_SZ	exacqVision Server
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 00 00 03 00 00 00 14 00...
ImagePath	REG_EXPAND_SZ	"C:\Program Files\exacqVision\Server\exacqd.exe"
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000010 (16)
WOW64	REG_DWORD	0x00000001 (1)

Edit String

Value name: ImagePath

Value data: "C:\Program Files\exacqVision\Server\exacqd.exe"

Initial Publication Date

March 28, 2019

Last Published Date

July 18, 2019

Resources

Please visit the Cyber Solutions Website to learn more about this security advisories.

Find out more about CVE-2019-7590 from NIST National Vulnerability Database (NVD), MITRE CVE® List , and ICSA-19-199-01 Johnson Controls exacqVision Server.

Sincerely,
Cyber Solutions