Talos Vulnerability Report

TALOS-2020-1184

Rockwell Automation RSLinx classic ethernet/IP server denial-of-service vulnerability

JANUARY 7, 2021

CVE NUMBER

CVE-2020-13573

Summary

A denial-of-service vulnerability exists in the Ethernet/IP server functionality of Rockwell Automation RSLinx Classic 2.57.00.14 CPR 9 SR 3. A specially crafted network request can lead to a denial of service. An attacker can send a sequence of malicious packets to trigger this vulnerability.

Tested Versions

Rockwell Automation RSLinx Classic 2.57.00.14 CPR 9 SR 3

Product URLs

https://lvmcc-pubs.rockwellautomation.com/pubs/LINX-TD001C-EN-P.pdf

CVSSv3 Score

7.5 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE

CWE-823 - Use of Out-of-range Pointer Offset

Details

RSLinx Classic software is a communication server for the MicroLogix 1100 Programmable Controller. It helps plant devices communicate with other Rockwell server and client applications.

The version used for the RSLinx Classic can be found within the MicroLogix 1100 (Programmable Controllers/MicroLogix) device. The vulnerability occurs when sending a Register Session request followed by a Send Unit Data message where the Address Item Length is smaller than the data that follows.

The following piece of code within the function at address `67a4bb10` has the vulnerability:

```
67a4bb4a                        xor     edx, edx  {0x0}
67a4bb4c                        pop     esi {__saved_esi}
67a4bb4d                        mov     dx, word [eax+0x2]
//Vulnerability happens here
67a4bb51                        lea     eax, [edx+eax+0x4]
67a4bb55                        mov     edx, dword [esp+0x10 {arg4}]
67a4bb59                        mov     dword [ecx], eax
//Crash happens here
67a4bb5b                        mov     ax, word [eax]
67a4bb5e                        mov     word [edx], ax
67a4bb61                        mov     eax, dword [ecx]
67a4bb63                        cmp     word [eax+0x2], 0x1
67a4bb68                        sbb     eax, eax
67a4bb6a                        and     eax, 0xc353
67a4bb6f                        retn    {__return_addr}
```

The vulnerability happens at address `67a4bb51`. EDX is the Address Item Length size, EAX points to the start of the Address Item and EAX+0x4 points to the start of the Address Item Data. At this point EDX is controlled by the user and since there is not a check that compares the user input size to make sure is less or equal than the application can receive and process. The resulting pointer points to unmapped memory and crashes when it gets dereferenced it as we see later in the code.

```
67a4bb51                        lea     eax, [edx+eax+0x4]
```

At this point edx, eax+0x4 contains the following:

edx:

```
0000beef  <-- Address Item Length
```

eax:

```
010e989c  ad de ef be 41 41 41 41-41 41 41 41 41 41 41 41  ....AAAAAAAAAAAA  <-- eax+0x4 points to Address Item Data
010e98ac  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
010e98bc  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
010e98cc  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
010e98dc  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
010e98ec  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
010e98fc  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
010e990c  41 41 41 41 41 41 41 41-41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
```

Which in byte length is 0x0898 and less than edx

The crash happens when dereferencing eax and moving it into ax, since [eax] points to [edx+eax+0x4], which the end result of the resulting pointer points to unmapped memory part and creates the crash.

```
67a4bb5b                      mov     ax, word [eax]
```

Crash Information

```
Executable search path is:
ModLoad: 00000000`00400000 00000000`00600000   C:\PROGRA~2\ROCKWE~1\RSLinx\RSLINX.EXE
ModLoad: 00007fff`18440000 00007fff`18630000   C:\WINDOWS\SYSTEM32\ntdll.dll
ModLoad: 00000000`76ed0000 00000000`7706a000   ntdll.dll
ModLoad: 00007fff`16c90000 00007fff`16ce5000   C:\WINDOWS\System32\wow64.dll
ModLoad: 00007fff`17f80000 00007fff`17ffd000   C:\WINDOWS\System32\wow64win.dll
ModLoad: 00000000`76ec0000 00000000`76ec9000   C:\WINDOWS\System32\wow64cpu.dll
ModLoad: 00000000`766b0000 00000000`76790000   KERNEL32.dll
ModLoad: 00000000`763f0000 00000000`765ef000   KERNELBASE.dll
ModLoad: 00000000`746c0000 00000000`74b09000   SETUPAPI.dll
ModLoad: 00000000`75e20000 00000000`75edf000   msvcrt.dll
ModLoad: 00000000`760e0000 00000000`7611b000   CFGMGR32.dll
ModLoad: 00000000`75200000 00000000`7531f000   ucrtbase.dll
ModLoad: 00000000`765f0000 00000000`766ab000   RPCRT4.dll
ModLoad: 00000000`74690000 00000000`746b5000   SspiCli.dll
ModLoad: 00000000`74680000 00000000`7468a000   CRYPTBASE.dll
ModLoad: 00000000`750e0000 00000000`7513f000   bcryptPrimitives.dll
ModLoad: 00000000`76a80000 00000000`76af6000   SECHOST.dll
ModLoad: 00000000`75f60000 00000000`75f79000   bcrypt.dll
ModLoad: 00000000`76b50000 00000000`76ce8000   USER32.dll
ModLoad: 00000000`75320000 00000000`75337000   win32u.dll
ModLoad: 00000000`76e90000 00000000`76eb1000   GDI32.dll
ModLoad: 00000000`76210000 00000000`7636c000   gdi32full.dll
ModLoad: 00000000`757e0000 00000000`7585c000   msvcp_win.dll
ModLoad: 00000000`767f0000 00000000`76869000   ADVAPI32.dll
ModLoad: 00000000`758a0000 00000000`75e1a000   SHELL32.dll
ModLoad: 00000000`76120000 00000000`761a4000   SHCORE.dll
ModLoad: 00000000`75340000 00000000`755b5000   combase.dll
ModLoad: 00000000`74b10000 00000000`750d1000   Windows.Storage.dll
ModLoad: 00000000`76e70000 00000000`76e8b000   profapi.dll
ModLoad: 00000000`76b00000 00000000`76b43000   POWRPROF.dll
ModLoad: 00000000`763e0000 00000000`763ed000   UMPDC.dll
ModLoad: 00000000`756d0000 00000000`75714000   SHLWAPI.dll
ModLoad: 00000000`756c0000 00000000`756cf000   AppCore.dll
ModLoad: 00000000`75870000 00000000`75883000   CRYPTSP.dll
ModLoad: 00000000`755c0000 00000000`756b7000   ole32.dll
ModLoad: 00000000`769e0000 00000000`76a72000   OLEAUT32.dll
ModLoad: 00000000`67d90000 00000000`67dbd000   rslinxnt.dll
ModLoad: 00000000`67cc0000 00000000`67cc8000   UTIL.dll
ModLoad: 00000000`742e0000 00000000`742e8000   VERSION.dll
ModLoad: 00000000`10000000 00000000`1036e000   RSwd32.dll
ModLoad: 00000000`75720000 00000000`757d0000   COMDLG32.dll
ModLoad: 00000000`6cb60000 00000000`6cb84000   WINMM.dll
ModLoad: 00000000`719b0000 00000000`719bf000   WTSAPI32.dll
ModLoad: 00000000`67ea0000 00000000`67f8c000   ENGINE.dll
ModLoad: 00000000`67e50000 00000000`67e57000   LOGGER.dll
ModLoad: 00000000`68ea0000 00000000`68fc4000   MFC42.dll
ModLoad: 00000000`71720000 00000000`717ad000   COMCTL32.dll
ModLoad: 00000000`68e30000 00000000`68ea0000   msvcp60.dll
ModLoad: 00000000`67e60000 00000000`67e94000   LINXCOMM.DLL
ModLoad: 00000000`71990000 00000000`719a3000   NETAPI32.dll
ModLoad: 00000000`6e4f0000 00000000`6e4f8000   WSOCK32.dll
ModLoad: 00000000`761b0000 00000000`7620e000   WS2_32.dll
ModLoad: 00000000`6c6f0000 00000000`6c713000   WINMMBASE.dll
ModLoad: 00000000`00ac0000 00000000`00b49000   IC32CKIT.dll
ModLoad: 00000000`68dc0000 00000000`68e2b000   WINSPOOL.DRV
ModLoad: 00000000`6e510000 00000000`6e5d6000   PROPSYS.dll
ModLoad: 00000000`710e0000 00000000`71112000   IPHLPAPI.DLL
ModLoad: 00000000`53400000 00000000`53403000   icmp.dll
ModLoad: 00000000`70fe0000 00000000`70ff1000   NAPINSP.dll
ModLoad: 00000000`70fc0000 00000000`70fd6000   PNRPNSP.dll
ModLoad: 00000000`70f60000 00000000`70fb2000   MSWSOCK.dll
ModLoad: 00000000`70ec0000 00000000`70f54000   DNSAPI.dll
ModLoad: 00000000`75890000 00000000`75897000   NSI.dll
ModLoad: 00000000`70eb0000 00000000`70ebb000   WINRNR.dll
ModLoad: 00000000`70e90000 00000000`70ea6000   nlaapi.dll
ModLoad: 00000000`70e80000 00000000`70e90000   wshbth.dll
ModLoad: 00000000`01030000 00000000`0104c000   Rstag32.dll
ModLoad: 00000000`75ee0000 00000000`75f60000   CLBCatQ.DLL
ModLoad: 00000000`3f230000 00000000`3f308000   RSTOP.DLL
ModLoad: 00000000`49000000 00000000`49070000   RSPROJ.DLL
ModLoad: 00000000`73c70000 00000000`73c78000   msiltcfg.dll
ModLoad: 00000000`73910000 00000000`73c6e000   msi.dll
ModLoad: 00000000`73700000 00000000`7390f000   COMCTL32.dll
ModLoad: 00000000`736d0000 00000000`736f6000   srpapi.dll
ModLoad: 00000000`75f80000 00000000`7607b000   CRYPT32.dll
ModLoad: 00000000`757d0000 00000000`757de000   MSASN1.dll
ModLoad: 00000000`74620000 00000000`74672000   mscoree.dll
ModLoad: 00000000`74410000 00000000`7449d000   mscoreei.dll
ModLoad: 00000000`723d0000 00000000`723e3000   fusion.dll
ModLoad: 00000000`72ef0000 00000000`736a0000   clr.dll
ModLoad: 00000000`723b0000 00000000`723c4000   VCRUNTIME140_CLR0400.dll
ModLoad: 00000000`72300000 00000000`723ab000   ucrtbase_clr0400.dll
ModLoad: 00000000`48000000 00000000`4807b000   RSReg.dll
ModLoad: 00000000`67a30000 00000000`67a8a000   ABTCP.drv
ModLoad: 00000000`69880000 00000000`69886000   RPCNS4.dll
ModLoad: 00000000`02d70000 00000000`02d9c000   RSTopsrv.DLL
ModLoad: 00000000`76380000 00000000`763de000   coml2.dll
ModLoad: 00000000`03090000 00000000`0319c000   FTCrypt.DLL
ModLoad: 00000000`74580000 00000000`7460e000   MSVCP90.dll
ModLoad: 00000000`744d0000 00000000`74573000   MSVCR90.dll
ModLoad: 00000000`68d90000 00000000`68db3000   DEVOBJ.dll
ModLoad: 00000000`76cf0000 00000000`76d36000   WINTRUST.dll
(1f20.1c14): Break instruction exception - code 80000003 (first chance)
ntdll!DbgBreakPoint:
00007fff`184dfaa0 cc              int     3
0:018> g
RPC:  Using rpcns4.dll.  The dll is no longer supported.
RPC:  Using rpcns4.dll.  The dll is no longer supported.
RPC:  Using rpcns4.dll.  The dll is no longer supported.
RPC:  Using rpcns4.dll.  The dll is no longer supported.
RPC:  Using rpcns4.dll.  The dll is no longer supported.
RPC:  Using rpcns4.dll.  The dll is no longer supported.
RPC:  Using rpcns4.dll.  The dll is no longer supported.
(1f20.ea8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
ABTCP!CMovingAveragePerSecond::`default constructor closure'+0x19dfb:
67a4bb5b 668b00          mov     ax,word ptr [eax]        ds:002b:0121578f=????
0:018:x86> r
eax=0121578f ebx=01208e10 ecx=03fafe98 edx=03fafea0 esi=01208980 edi=0120987c
eip=67a4bb5b esp=03fafe7c ebp=03faff30 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
```

```
ABTCP!CMovingAveragePerSecond::`default constructor closure'+0x19dfb:
67a4bb5b 668b00          mov     ax,word ptr [eax]        ds:002b:0121578f=????
```

Timeline

2020-10-23 - Vendor Disclosure

2020-10-26 - Talos issued copy of advisory report

2020-12-14 - Follow up with vendor

2021-01-05 - 75 day follow up with vendor; Vendor acknowledged issue resolved 2020-11-04

2021-01-07 - Public Release

CREDIT

Discovered by Alexander Perez-Palma of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1163

NEXT REPORT TALOS-2020-1190