tenable

CODESYS V3 Unauthenticated Remote Heap Overflow

Critical

← View More Research Advisories

Synopsis

A heap overflow vulnerability exists in CmpWebServerHandlerV3.dll (file version 3.5.15.20) due to improper validation of user-supplied data sent to the CODESYS V3 web server URL endpoint /WebVisuV3.

The flaw is due to the fact that the MemGCGetSize function adds 0x5c bytes to the requested allocation size during memory allocation operation:

```
__wibu00:004BF8C0 MemGCGetSize proc near              ; CODE XREF: SysMemAllocCode+39↓p
__wibu00:004BF8C0                                     ; SysMemAllocData+1B↓p
__wibu00:004BF8C0                                     ; SysMemReallocData+3C↓p
__wibu00:004BF8C0                                     ; DATA XREF: __wibu01:00813B28↓o
__wibu00:004BF8C0
__wibu00:004BF8C0 arg_size  = dword ptr  8
__wibu00:004BF8C0
__wibu00:004BF8C0           push    ebp
__wibu00:004BF8C1           mov     ebp, esp
__wibu00:004BF8C3           mov     eax, [ebp+arg_size]; attacker-controlled
__wibu00:004BF8C6           add     eax, 5Ch ; '\'    ; int32 overflow!
__wibu00:004BF8C6                                     ; i.e., size can be 0xffffffff
__wibu00:004BF8C9           pop     ebp
__wibu00:004BF8CA           retn
__wibu00:004BF8CA MemGCGetSize endp
```

The extra 0x5c bytes appears to be used for memory garbage collection purposes. The MemGCGetSize function is called within the SysMemAllocData function, which is used by many CODESYS components to allocate memory from the heap.

An unauthenticated, remote attacker can request a very large memory allocation size (i.e., 0xffffffff) via a WEB_CLIENT_OPENCONNECTION message sent to the CmpWebServerHandlerV3 component:

```
|foo|-1|true|
```

The CmpWebServerHandlerV3 component (when in state 0) attempts to allocate -1 (0xffffffff) bytes for the communication buffer. When the SysMemAllocData function is called, the memory allocation size gets overflowed and a small (0xffffffff + 0x5c = 0x5b) heap buffer is actually allocated.

The attacker then sends a WEB_CLIENT_RUN_SERVICE message to overflow the small communication buffer:

```
.text:100039F4          call    HandleVisuService
.text:100039FA          add     esp, 14h
.text:100039FD          mov     [ebp+err], eax
.text:10003A00          cmp     [ebp+err], 0
.text:10003A04          jnz     short err_10003A54
.text:10003A06          mov     ecx, [ebp+HdrSizePlus4] ; attacker-controlled
.text:10003A09          push    ecx
.text:10003A0A          mov     edx, [ebp+pbLayer7] ; attacker-controlled
.text:10003A0D          push    edx
.text:10003A0E          mov     eax, [ebp+cbCommBuf2] ; ffffffff
.text:10003A11          push    eax
.text:10003A12          mov     ecx, [ebp+pbCommBuf2] ; very small buf => heap buf overflow!
.text:10003A15          push    ecx
.text:10003A16          call    CMUtlSafeMemCpy
```

The following windbg output shows 0x4014 bytes of attacker-controlled data is being copied to a 0x3-byte (0x5b - (0x0028c3d8 - 0x0028c380) = 3) user buffer on the heap:

```
CmpWebServerHandlerV3!ComponentEntry+0x1d66:
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:\Program Files\CODESYS 3.5.15.20\GatewayPLC\CODESYSControlService.exe -
01b13a16 ff152c85b101    call    dword ptr [CmpWebServerHandlerV3!ComponentEntry+0x687c (01b1852c)] ds:0023:01b1852c=00566110
0:013> dd esp L4
0460fddc  0028c3d8 ffffffff 023107ac 00004014
0:013> !heap -p -a 0028c3d8
    address 0028c3d8 found in
    _HEAP @ 260000
      HEAP_ENTRY Size Prev Flags    UserPtr UserSize - state
        0028c378 000d 0000  [00]   0028c380    0005b - (busy)
```

The attached PoC can be used to terminate a 32-bit CODESYSControlService.exe:

```
   python codesys_v3_webserver_int32_overflow.py  8080
```

Note that when running the PoC, it's important that the CmpWebServerHandlerV3 component must be in 'state' 0. When CODESYSControlService.exe starts, CmpWebServerHandlerV3 is in state 0.

Solution

Upgrade to V3.5.15.40.

Proof of Concept

Disclosure Timeline

12/02/2019 - Vulnerability discovered
12/11/2019 - Vendor Informed, 90 Days is 3/10/2020
12/11/2019 - CODESYS acknowledges. Asks how we would like to be acknowledged.
12/11/2019 - "Tenable, Inc."
12/11/2019 - CODESYS asks for clarification on 90-day date.
12/11/2019 - Tenable clarifies.
01/28/2020 - Vendor informs that they plan to release the patch in the middle of March.
03/18/2020 - CODESYS informs us that due to COVID-19, they will need to postpone their patch and advisory by a few days. They however do plan to release version 3.5.15.40 in mid March.
03/25/2020 - CODESYS has released an advisory and bug fix.

Risk Information

CVE ID: CVE-2020-10245
Tenable Advisory ID: TRA-2020-16
CVSSv2 Base / Temporal Score: 10.0 / 7.8
CVSSv2 Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Affected Products:
According to CODESYS, "all CODESYS V3 runtime systems containing the web server (CmpWebServer and CmpWebServerHandler) in all versions prior V3.5.15.40 are affected." Please see advisory for specifics.
Risk Factor: Critical

Advisory Timeline

03/25/2020 - Advisory released

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
Media