tenable

CODESYS V3 Unauthenticated Webserver Memory Leak DoS

High

← View More Research Advisories

Synopsis

A memory leak condition exists in CODESYSControlService.exe (file version 3.5.15.40) due to failure to free heap-based memory buffers when handling a layer 7, SRV_VISU_REGISTERCLIENT request sent to web server URL endpoint /WebVisuV3. An unauthenticated, remote attacker can exploit this issue, via a series of specially crafted HTTP requests, to increase memory usage in the process which can potentially result in denial of service of the CODESYS V3 runtime system.

In the SRV_VISU_REGISTERCLIENT request, the attacker can specify more than one binary tags. The CmpVisuServer component in the runtime allocates a buffer from the heap to store certain data in a binary tag and stores the buffer pointer in a field of some structure:

```
__wibu00:0053FB9E      mov     ecx, [ebp+arg_pOut]
__wibu00:0053FBA1      imul    edx, [ecx+ST14.nItems], 2Ch
__wibu00:0053FBA5      push    edx
__wibu00:0053FBA6      push    offset aCmpvisuserver ; "CmpVisuServer"
__wibu00:0053FBAB      call    SysMemAllocData
__wibu00:0053FBB0      add     esp, 0Ch
__wibu00:0053FBB3      mov     ecx, [ebp+arg_pOut]
__wibu00:0053FBB6      mov     [ecx+ST14.pItems], eax
```

When a subsequent binary tag is processed, another memory buffer is allocated but its pointer is stored in the same location, overwriting the pointer for the previously allocated buffer. When the processing of the SRV_VISU_REGISTERCLIENT request is done, only the last buffer is freed:

```
__wibu00:0053D361 mov eax, [ebp+ST14.pItems]
 __wibu00:0053D367 push eax
 __wibu00:0053D368 push offset aCmpvisuserver ; "CmpVisuServer"
 __wibu00:0053D36D call SysMemFreeData
```

The issue can be summed up as:

```
for (i = 0; i < num_binary_tags; i++)
{
st14->pItems = SysMemAllocData(...,nItems * 0x2C,...);
}
...
SysMemFreeData(...,st14->pItems);
```

The SRV_VISU_REGISTERCLIENT request is carried in an HTTP header and it appears there is a maximum size (i.e., 48K) for HTTP headers. So the attacker may need to send a large of number requests in order to leak memory to a point where CODESYS runtime components may no longer able to allocate memory for their respective functionalities.

It appears that CODESYSControlService.exe employs some sort of memory garbage collection system, where allocated memory that is no longer in use can be freed. However, the attacker is still able to cause memory allocation failure as indicated in the log file:

```
2020-04-28T22:37:46Z, 0x00000054, 2, 0, 9, !!!! Warning: VisuInfoTuple not found for RegisterClient, ExtId: 376465, Application=APP
 2020-04-28T22:37:46Z, 0x00000057, 4, 0, 0, **** ERROR: Allocation of clienttags failed 576
 2020-04-28T22:37:46Z, 0x00000054, 2, 0, 9, !!!! Warning: VisuInfoTuple not found for RegisterClient, ExtId: 376467, Application=APP
 2020-04-28T22:37:46Z, 0x00000057, 4, 0, 0, **** ERROR: Allocation of clienttags failed 576
 2020-04-28T22:37:46Z, 0x00000054, 2, 0, 9, !!!! Warning: VisuInfoTuple not found for RegisterClient, ExtId: 376469, Application=APP
 2020-04-28T22:37:46Z, 0x00000057, 4, 0, 0, **** ERROR: Allocation of clienttags failed 576
 2020-04-28T22:37:46Z, 0x00000054, 2, 0, 9, !!!! Warning: VisuInfoTuple not found for RegisterClient, ExtId: 376471, Application=APP
 2020-04-28T22:37:46Z, 0x00000057, 4, 0, 0, **** ERROR: Allocation of clienttags failed 576
 2020-04-28T22:37:46Z, 0x00000054, 2, 0, 9, !!!! Warning: VisuInfoTuple not found for RegisterClient, ExtId: 376473, Application=APP
 2020-04-28T22:37:46Z, 0x00000057, 4, 0, 0, **** ERROR: Allocation of clienttags failed 576
 ...
```

Proof of Concept

codesys_v3_webserver_memory_leak_dos_tra_2020_46.py

Solution

Upgrade to V3.5.16.10.

Additional References

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=

Disclosure Timeline

04/28/2020 - Vulnerability discovered
05/01/2020 - Vulnerability reported to CODESYS. 90-day date is July 30, 2020.
05/07/2020 - CODESYS acknowledges. Asks how we would like to be credited.
05/07/2020 - Tenable replies and provides Python poc again.
05/07/2020 - CODESYS acknowledges.
05/21/2020 - Tenable asks for an update.

06/22/2020 - Tenable thanks CODESYS.
07/22/2020 - CODESYS notifies Tenable of their security advisory.

Risk Information

CVE ID: CVE-2020-15806
Tenable Advisory ID: TRA-2020-46
CVSSv2 Base / Temporal Score: 7.8 / 6.1
CVSSv2 Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C
CVSSv3 Base / Temporal Score: 8.6 / 7.7
CVSSv3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
Affected Products:
All CODESYS V3 runtime systems in all versions before V3.5.16.10. Please see the CODESYS advisory for more specific information on affected systems.
Risk Factor: High

Advisory Timeline

07/22/2020 - Advisory published.

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media