CODESYS V3 Denial of Service

High

← View More Research Advisories

Synopsis

When the CODESYS V3 runtime allocates memory for channel buffers, it reads the MaxChannels and BufferSize settings under the [CmpChannelServer] section in the configuration file (i.e., CODESYSControl.cfg, Gateway.cfg). The integer settings in the configuration file are treated as signed int32. If BufferSize is a large positive number (i.e, 0x7fffffff) and MaxChannels * 2 is a negative number (i.e., MaxChannels = 0x7fffffff), it will cause the runtime to allocate a large number of bytes (i.e., 0x7ffff008) from the heap. This could cause SysMemAllocData() to fail, resulting in an error in the log:

```
01571694396373, 0x0000000a, 4, 17, 0, Failed to allocate memory for channel buffers, no communication channels available
```

When the channel layer (layer 4) is not available, layer 7 services cannot be run, severely limiting the runtime functionalities.

Additionally, we reported a bug that CODESYS has deemed to be an improvement:

GatewayService.exe implements layer 7 service group 6, which allows manipulation (i.e., get, set, remove operations) of settings in the gateway configuration file. To access the layer 7 services, a valid session ID is required. It looks like an unauthenticated, remote attacker could login as an anonymous user to obtain a session ID. On a PLC (i.e., CODESYSControlService.exe) that also implements service group 6, the CmpUserMgr component is seen to be included in the runtime to prevent anonymous access. However, it does not appear the CmpUserMgr component is implemented in GatewayService.exe. So it's unclear whether GatewayService.exe can be configured to prevent an unauthenticated remote attacker from changing the configuration file.

When combining both issues, an unauthenticated remote attacker can cause a DoS on GatewayService.exe when it restarts.

The attached PoC attempts to write the following settings to Gateway.cfg:

```
[CmpChannelServer]
MaxChannels=2147483647
BufferSize=2147483647
```

Solution

Upgrade to V3.5.15.30.

Proof of Concept

https://github.com/tenable/poc/blob/master/codesys/codesys_gateway_v3_config_modification_tra_2020_04.py

Additional References

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=

Disclosure Timeline

10/29/2019 - Tenable reports vulnerabilities. 90-day date is 01/28/2020.
10/31/2019 - CODESYS will investigate. Asks if we would like to be acknowledged in the same fashion as last time.
10/31/2019 - Tenable acknowledges. This is fine.
11/19/2019 - Tenable asks for an update.
11/20/2019 - CODESYS says they are still investigating.
11/20/2019 - Tenable thanks CODESYS for update.
12/03/2019 - Tenable asks for an update.
12/05/2019 - CODESYS is "on track". They have scheduled a fix internally, and they will provide an updated timeline just before Christmas.
12/05/2019 - Tenable acknowledges.
12/19/2019 - CODESYS will fix the "Negative MaxChannels DoS" in the next patch release. The other bug is considered an improvement and not a vulnerability, so it will be fixed in the next main version. They will provide the advisory as soon as it is avail
12/19/2019 - Tenable asks for the anticipated advisory release date.
01/09/2020 - Tenable follows up.
01/09/2020 - CODESYS plans to release a fix and advisory around Jan 28.
01/21/2020 - Tenable follows up.
01/22/2020 - CODESYS has a release scheduled for 1/24. They will send a link to their advisory as soon as it is public.
01/22/2020 - Tenable acknowledges. We will publish our advisory once the patch is public.
01/23/2020 - CODESYS notifies tenable of advisory and bug fix releases.

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

CVSSv2 Base / Temporal Score: 7.8 / 6.1
CVSSv2 Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Affected Products: All affected products prior to 3.5.15.30 listed in the CODESYS 2020-01 advisory.
Risk Factor: High

Advisory Timeline

01/23/2020 - Advisory released

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