Talos Vulnerability Report

TALOS-2021-1305

CODESYS Development System ObjectManager.plugin Project.get_MissingTypes() Unsafe Deserialization vulnerability

JULY 26, 2021

CVE NUMBER

CVE-2021-21868

Summary

An unsafe deserialization vulnerability exists in the ObjectManager.plugin Project.get_MissingTypes() functionality of CODESYS GmbH CODESYS Development System 3.5.16 and 3.5.17. A specially crafted file can lead to arbitrary command execution. An attacker can provide a malicious file to trigger this vulnerability.

Tested Versions

CODESYS GmbH CODESYS Development System 3.5.16
CODESYS GmbH CODESYS Development System 3.5.17

Product URLs

https://store.codesys.com/codesys.html

CVSSv3 Score

8.8 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CWE

CWE-502 - Deserialization of Untrusted Data

Details

The CODESYS Development System is the IEC 61131-3 programming tool for industrial control and automation technology, available in 32- and a 64-bit versions.

Unsafe deserialization occurs within GetMissingTypesFromAuxStream() on the ObjectStream class.

```
private IList<T> GetMissingTypesFromAuxStream<T>(string stAuxilaryName)
{
    ChunkedMemoryStream chunkedMemoryStream = new ChunkedMemoryStream();
    APEnvironment.ObjectMgr.GetAuxiliaryFileEntry(this._nProjectHandle, stAuxilaryName, chunkedMemoryStream);
    chunkedMemoryStream.Position = 0L;
    return (IList<T>)((IFormatter)new BinaryFormatter()).Deserialize(chunkedMemoryStream);  // [1]
}
```

The `BinaryFormatter.Deserialize` method is never safe when used with untrusted input [2]. The deserialization that occurs at [1] is vulnerable to exploitation via the missingtypeinformation.auxiliary file within a project.

[2] https://docs.microsoft.com/en-us/dotnet/standard/serialization/binaryformatter-security-guide

Crash Information

Partial Call Stack

```
objectmanager.plugin.dll!_3S.CoDeSys.ObjectManager.Project.GetMissingTypesFromAuxStream<_3S.CoDeSys.Core.Objects.MissingTypeInformation2>
(string stAuxilaryName = "MissingTypeInformation")
objectmanager.plugin.dll!_3S.CoDeSys.ObjectManager.Project.MissingTypes.get()
objectmanager.plugin.dll!_3S.CoDeSys.ObjectManager.ObjectManager.InspectAndLoadProject(System.IO.Stream stream = {System.IO.MemoryStream},
string stStreamName = "Untitled3", string stWorkingFolder = @"C:\ProgramData\CODESYS\Temporary Files\150827c2-3d17-49b3-bfde-d666a3011711",
string stProjectPath = @"C:\Users\User\Documents\Untitled3.project", _3S.CoDeSys.Core.Objects.IProjectInspectionReporter reporter =
{ns2.Class57}, out int nProjectHandle = 0xFFFFFFFF)
engine.plugin.dll!ns1.Class60._3S.CoDeSys.Core.IProjects4.OpenProject(string stPath = @"C:\Users\User\Documents\Untitled3.project", bool
immediatelyUpgradeStorageFormat = false, params System.Guid[] projectAttrs = {System.Guid[0x00000002]})
engine.plugin.dll!ns1.Class60._3S.CoDeSys.Core.IProjects.OpenProject(string stPath = @"C:\Users\User\Documents\Untitled3.project", params
System.Guid[] projectAttrs = {System.Guid[0x00000002]}) (IL≈0x0000, Native=0x00007FFD7A8BA950+0x3E)
filecommands.plugin.dll!_3S.CoDeSys.FileCommands.FileCommandHelper.OpenProject(string stPath = @"C:\Users\User\Documents\Untitled3.project",
bool readOnly = false, System.Guid converterOrFilterGuid = {System.Guid})
filecommands.plugin.dll!_3S.CoDeSys.FileCommands.FileOpenCommand.ExecuteBatch(string[] arguments = {string[0x00000003]})
```

Serialization Exception

when opening a project with randomly modified bytes in the missingtypeinformation.auxiliary file.

```
 {System.Runtime.Serialization.SerializationException: The input stream is not a valid binary format. The starting contents (in bytes) are:
64-73-61-73-69-6F-6E-0F-4F-77-6E-69-6E-67-50-61-63 ...
 at System.Runtime.Serialization.Formatters.Binary.SerializationHeaderRecord.Read(__BinaryParser input)
 at System.Runtime.Serialization.Formatters.Binary.__BinaryParser.ReadSerializationHeaderRecord()
 at System.Runtime.Serialization.Formatters.Binary.__BinaryParser.Run()
 at System.Runtime.Serialization.Formatters.Binary.ObjectReader.Deserialize(HeaderHandler handler, __BinaryParser serParser, Boolean fCheck,
Boolean isCrossAppDomain, IMethodCallMessage methodCallMessage)
 at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream, HeaderHandler handler, Boolean
fCheck, Boolean isCrossAppDomain, IMethodCallMessage methodCallMessage)
 at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream, HeaderHandler handler, Boolean
fCheck, IMethodCallMessage methodCallMessage)
 at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream, HeaderHandler handler, Boolean
fCheck)
 at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream, HeaderHandler handler)
 at System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(Stream serializationStream)
 at _3S.CoDeSys.ObjectManager.Project.GetMissingTypesFromAuxStream[T](String stAuxilaryName)
 at _3S.CoDeSys.ObjectManager.Project.get_MissingTypes()
 at _3S.CoDeSys.ObjectManager.ObjectManager.InspectAndLoadProject(Stream stream, String stStreamName, String stWorkingFolder, String
stProjectPath, IProjectInspectionReporter reporter, Int32& nProjectHandle)}     System.Runtime.Serialization.SerializationException


{================================================================================
  Project: 0
================================================================================
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Object Manager:
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Device - _3S.CoDeSys.DeviceObject.DeviceObject - {3e5778ec-f151-4a52-b153-30a9170220d4}
  Plc Logic - _3S.CoDeSys.PlcLogicObject.PlcLogicObject - {89b74c99-ab25-401a-a5d6-76dc5ca0ad24}
    Application - _3S.CoDeSys.ApplicationObject.ApplicationObject - {03bc6468-4e62-473e-971c-9bf8185afe04}
      Library Manager - _3S.CoDeSys.LibManObject.LibManObject - {ba4f739b-e1fb-44ff-a7b7-0513322c4f40}
Project Settings - _3S.CoDeSys.Engine.WorkspaceObject - {6470a90f-b7cb-43ac-9ae5-94b2338b4573}
Library Manager - _3S.CoDeSys.LibManObject.LibManObject - {a9964481-f634-4b4a-aced-6fa9cb55a8fe}

}
```

Timeline

2021-05-18 - Vendor Disclosure

2021-07-26 - Public Release

CREDIT

Discovered by Patrick DeSantis of Cisco Talos.
