Talos Vulnerability Report

TALOS-2021-1306

CODESYS Development System Engine.plugin ProfileInformation ProfileData Unsafe Deserialization vulnerability

JULY 26, 2021

CVE NUMBER

CVE-2021-21869

Summary

An unsafe deserialization vulnerability exists in the Engine.plugin ProfileInformation ProfileData 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 ProfileData[] in the ProfileInformation class.

```
[DefaultSerialization("Profile")]
[StorageVersion("3.3.0.0")]

private byte[] ProfileData
{
    get
    {
        byte[] result;
        using (ChunkedMemoryStream chunkedMemoryStream = new ChunkedMemoryStream())
        {
            new BinaryFormatter
            {
                Binder = new LegacyCODESYSSerializationBinder()
            }.Serialize(chunkedMemoryStream, this.profile_0);
            result = chunkedMemoryStream.ToArray();
        }
        return result;
    }
    set
    {
        using (ChunkedMemoryStream chunkedMemoryStream = new ChunkedMemoryStream(value))
        {
            BinaryFormatter binaryFormatter = new BinaryFormatter();
            this.profile_0 = (Profile)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 profile.auxiliary file within a project.

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

Crash Information

Call Stack

```
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.__BinaryParser.ReadObjectWithMapTyped(System.Runtime.Serialization.Formatters.Bi
nary.BinaryObjectWithMapTyped record = {System.Runtime.Serialization.Formatters.Binary.BinaryObjectWithMapTyped})
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.__BinaryParser.ReadObjectWithMapTyped(System.Runtime.Serialization.Formatters.Bi
nary.BinaryHeaderEnum binaryHeaderEnum = ObjectWithMapTypedAssemId)
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.__BinaryParser.Run()
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.ObjectReader.Deserialize(System.Runtime.Remoting.Messaging.HeaderHandler handler
= null, System.Runtime.Serialization.Formatters.Binary.__BinaryParser serParser =
{System.Runtime.Serialization.Formatters.Binary.__BinaryParser}, bool fCheck = true, bool isCrossAppDomain = false,
System.Runtime.Remoting.Messaging.IMethodCallMessage methodCallMessage = null)
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(System.IO.Stream serializationStream =
{_3S.CoDeSys.Utilities.ChunkedMemoryStream}, System.Runtime.Remoting.Messaging.HeaderHandler handler = null, bool fCheck = true, bool
isCrossAppDomain = false, System.Runtime.Remoting.Messaging.IMethodCallMessage methodCallMessage = null)
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(System.IO.Stream serializationStream =
{_3S.CoDeSys.Utilities.ChunkedMemoryStream}, System.Runtime.Remoting.Messaging.HeaderHandler handler = null, bool fCheck = true,
System.Runtime.Remoting.Messaging.IMethodCallMessage methodCallMessage = null)
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(System.IO.Stream serializationStream =
{_3S.CoDeSys.Utilities.ChunkedMemoryStream}, System.Runtime.Remoting.Messaging.HeaderHandler handler = null, bool fCheck = true)
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(System.IO.Stream serializationStream =
{_3S.CoDeSys.Utilities.ChunkedMemoryStream}, System.Runtime.Remoting.Messaging.HeaderHandler handler = null)
mscorlib.dll!System.Runtime.Serialization.Formatters.Binary.BinaryFormatter.Deserialize(System.IO.Stream serializationStream =
{_3S.CoDeSys.Utilities.ChunkedMemoryStream})
engine.plugin.dll!_3S.CoDeSys.Engine.ProfileInformation.ProfileData.set(byte[] value = {byte[0x00004CEF]})
[Lightweight Function]
objectmanager.plugin.dll!_3S.CoDeSys.ObjectManager.GenericObjectService.SetSerializableValueImpl(_3S.CoDeSys.Core.Objects.GenericObject go =
{_3S.CoDeSys.Engine.ProfileInformation}, _3S.CoDeSys.ObjectManager.TypeAccess typeAccess = {_3S.CoDeSys.ObjectManager.TypeAccess}, string
valueName = "Profile", object value = {byte[0x00004CEF]})
objectmanager.plugin.dll!_3S.CoDeSys.ObjectManager.GenericObjectService.SetSerializableValue(_3S.CoDeSys.Core.Objects.GenericObject go =
{_3S.CoDeSys.Engine.ProfileInformation}, string valueName = "Profile", object value = {byte[0x00004CEF]})
Objects.dll!_3S.CoDeSys.Core.Objects.GenericObject.SetSerializableValue(string stValueName = "Profile", object value = {byte[0x00004CEF]})
binaryarchive.plugin.dll!ns3.Class4.method_9(System.IO.BinaryReader binaryReader_0 = {System.IO.BinaryReader}, ns6.Class6 class6_0 =
{ns6.Class6}, bool bool_0 = true)
binaryarchive.plugin.dll!ns3.Class4.method_1(System.IO.BinaryReader binaryReader_0 = {System.IO.BinaryReader}, bool bool_0 = true, out
string string_0 = null)
binaryarchive.plugin.dll!ns3.Class4.imethod_0(System.IO.BinaryReader binaryReader_0 = {System.IO.BinaryReader},
_3S.CoDeSys.Core.Objects.IArchivable iarchivable_0 = null, byte[] byte_0 = null, bool bool_0 = true, out string string_0 = null)
binaryarchive.plugin.dll!_3S.CoDeSys.BinaryArchive.BinaryArchiveReader.Load()
binaryarchive.plugin.dll!_3S.CoDeSys.BinaryArchive.BinaryArchiveReader.Fill(_3S.CoDeSys.Core.Objects.IArchivable obj =
{_3S.CoDeSys.ObjectManager.ProfileInformation})
objectmanager.plugin.dll!_3S.CoDeSys.ObjectManager.Project.Load(System.IO.Stream stream = {System.IO.MemoryStream}, string stStreamName =
"profile")
objectmanager.plugin.dll!_3S.CoDeSys.ObjectManager.ObjectManager.InspectAndLoadProject(System.IO.Stream stream = {System.IO.MemoryStream},
string stStreamName = "profile", string stWorkingFolder = @"C:\ProgramData\CODESYS\Temporary Files\9374fe72-1075-4e3c-927c-c77629334472",
string stProjectPath = @"C:\Users\User\Documents\codesys\projects_test\profile.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\codesys\projects_test\profile.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\codesys\projects_test\profile.project", params System.Guid[] projectAttrs = {System.Guid[0x00000002]})
filecommands.plugin.dll!_3S.CoDeSys.FileCommands.FileCommandHelper.OpenProject(string stPath =
@"C:\Users\User\Documents\codesys\projects_test\profile.project", bool readOnly = false, System.Guid converterOrFilterGuid = {System.Guid})
```

Serialization Exception

when opening a project with randomly modified bytes in the profile.auxiliary file and a missing profile7.auxiliary file.

```
StackTrace
at System.Runtime.Serialization.Formatters.Binary.__BinaryParser.ReadObjectWithMapTyped(BinaryObjectWithMapTyped record)
at System.Runtime.Serialization.Formatters.Binary.__BinaryParser.ReadObjectWithMapTyped(BinaryHeaderEnum binaryHeaderEnum)
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.Engine.ProfileInformation.set_ProfileData(Byte[] value)
at SetterP(Object , Object )
at _3S.CoDeSys.ObjectManager.GenericObjectService.SetSerializableValueImpl(GenericObject go, TypeAccess typeAccess, String valueName, Object
value)
at _3S.CoDeSys.ObjectManager.GenericObjectService.SetSerializableValue(GenericObject go, String valueName, Object value)
at _3S.CoDeSys.Core.Objects.GenericObject.SetSerializableValue(String stValueName, Object value)
at ns3.Class4.method_9(BinaryReader binaryReader_0, Class6 class6_0, Boolean bool_0)
at ns3.Class4.method_1(BinaryReader binaryReader_0, Boolean bool_0, String& string_0)
at ns3.Class4.imethod_0(BinaryReader binaryReader_0, IArchivable iarchivable_0, Byte[] byte_0, Boolean bool_0, String& string_0)
at _3S.CoDeSys.BinaryArchive.BinaryArchiveReader.Load()
at _3S.CoDeSys.BinaryArchive.BinaryArchiveReader.Fill(IArchivable obj)
at _3S.CoDeSys.ObjectManager.Project.Load(Stream stream, String stStreamName)
at _3S.CoDeSys.ObjectManager.ObjectManager.InspectAndLoadProject(Stream stream, String stStreamName, String stWorkingFolder, String
stProjectPath, IProjectInspectionReporter reporter, Int32& nProjectHandle)


+ this {=================================================================================
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}

=================================================================================
Project: 3
=================================================================================
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Object Manager:
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Project Settings - _3S.CoDeSys.Engine.WorkspaceObject - {6470a90f-b7cb-43ac-9ae5-94b2338b4573}

=================================================================================
Project: 4
=================================================================================
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Object Manager:
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Project Settings - _3S.CoDeSys.Engine.WorkspaceObject - {6470a90f-b7cb-43ac-9ae5-94b2338b4573}

} _3S.CoDeSys.ObjectManager.ObjectManager
```

Timeline

2021-05-18 - Vendor Disclosure

2021-07-26 - Public Release

CREDIT

Discovered by Patrick DeSantis of Cisco Talos.