Release Note CODESYS V3.5 SP15 Patch 4

25.03.2020

1 Release Notes

Key	Summary	Release Note	Component/s
CDS-68373	**Webvisu, Webserver:** PLC crashes with crafted request	**[[GENERAL]]** For more details see Advisory 2019-10, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-10_CDS-68341.pdf	CODESYS Control
CDS-68431	**WebServer:** Heap Buffer overflow vulnerability	**[[GENERAL]]** For more details see Advisory 2019-10, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-10_CDS-68341.pdf	Web Visualization
CDS-67712	**CODESYS Gateway Win32/x64:** Add Edge functionality	**[[GENERAL]]** We strongly recommend to replace all existing CODESYS Edge Gateway - BETA VERSIONs by the CODESYS Gateway V3.5.15.10 or higher.	Gateway Server
CDS-62029	Active content in **library documentation** may be used to execute hostile code	**[[GENERAL]]** For more details see Advisory 2019-05, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-05_CDS-62029.pdf JavaScript included in the library documentation is only executed anymore, if the library was sigend with a valid certificate.	CODESYS
CDS-63096	**Compiler, DevApp:** Persistent variable configuration is lost after import	**[[GENERAL]]** Applications which are removed are not automatically deleted from the persistent variable configuration anymore. Instead a new button is available which can be used to clear unknown or deleted applications manually from the persistent variable configuration.	CODESYS

CDS-63576	**Compiler:** No compile issue if a action and a fb_instance has the same name	**[[GENERAL]]** The new warning C0508 is reported when a local variable shadows a local method or action in a POU. Compilerversion >= 3.5.15.0	CODESYS
CDS-64543	**WebVisu:** Specific request crashes WebServer with an exception	**[[GENERAL]]** For more details see Advisory 2019-01, which is available on the CODESYS website: https://customers.CODESYS.com/fileadmin/data/customers/security/2019/Advisory2019-01_CDS-64543.pdf	CODESYS
CDS-65020	**BACnet**: CmpBACnet - wrong declaration of IEC_BACNET_STRING.UNION_BACNET_STRING.wstringData	**[[COMPATIBILITY_INFORMATION]]** Fixed wrong declaration of BACNET_STRING.data.wstringData. BACNET_STRING.data.wstringData is relevant for DBCS- and UCS-2 encoding, which are not supported right now. No matter of that, the problem needed to be fixed to prevent later API changes if those encodings should be supported in the future. Fixing BACNET_STRING results in API signature changes for bacnetreinitializedevice bacnetrestorebacnetdevice bacnetlifesafetyoperation bacnetconftextmessage bacnetunconftextmessage bacnetconfeventnotification bacnetdevicecommcontrol bacnetunconfeventnotification bacnetihaveex bacnetacknowledgealarm bacnetfindupdateobjectidnamebindings bacnetdeleteobjectidnamebindings bacnetbackupbacnetdevice bacnetdoesobjectnameexist bacnetacknowledgeinternalalarm bacnetwhohas bacnetwritegroup	CODESYS
CDS-65993	**BACnet:** CmpBACnet - remove BACnetReadPropertyConditional	**[[COMPATIBILITY_INFORMATION]]** ReadPropertyConditional has been removed from the standard so the according method BACnetReadPropertyConditional was removed from CmpBACnet.	CODESYS
CDS-47439	**SysFileWin32, SysFileOpen:** It should be possible to specify a share mode when opening a file	**[[COMPATIBILITY_INFORMATION-EndUser]]** SysFileDelete() under Windows (Control Win and Control RTE) works now, if the file is still opened!	CODESYS Control

		In this case the file will be deleted really on the filesystem, if the last open handle is closed on the file!	
CDS-51688	**Control Win:** Disable usage of multiple instances on one hardware	**[[COMPATIBILITY_INFORMATION-EndUser]]** License for CODESYS Control Win cannot be used anymore for several instances of the runtime! So the license is only valid for one instance.	CODESYS Control
CDS-54035	**CmpIoMgr:** Avoid long locks in ReadInputs / WriteOutputs	**[[COMPATIBILITY_INFORMATION-OEM]]** There is a new feature for IO-drivers to do the synchronization itself and not by the IoManager. NOTE: Exisiting IO-drivers worked like before! There is no change in the existing behavior! To use this feature, an IO-driver can specify the following new property: #define DRVPROP_NO_SYNC 0x0080 Two new interfaces in CmpIoMgrItf can be used afterwards to do own synchronization: - IoMgrLockEnter() - IoMgrLockLeave() See IoMgrItf for details.	CODESYS Control
CDS-56119	**Hilscher CIFX SDK - CmpHilscherCIFX:** Separation from the runtime kernel and move to Contrib repository	**[[COMPATIBILITY_INFORMATION-OEM]]** Hilscher cifX Toolkit is separated now from the runtime kernel files to: $\Components__Contrib__\HilscherCifxToolkit So perhaps your build process must be adapted here!	CODESYS Control
CDS-56660	**Update Hilscher CIFX** Toolkit to v1.4.0.0	**[[COMPATIBILITY_INFORMATION-OEM]]** Hilscher cifX toolkit is upgraded now to v1.4.0.0! Additionally the CIFX_TOOLKIT_PARAMETER_CHECK is enabled by default (see OS_Includes.h)! Can be disabled with the macro CIFX_TOOLKIT_PARAMETER_CHECK_DISABLE.	CODESYS Control

CDS-60925	**CAAFile:** issues with Exclusive mode of FILE.open	**[[COMPATIBILITY_INFORMATION-EndUser]]** Parameter xExclusive in CAA_File.library::Open functionblock cannot be supported, because our targets only support POSIX behaviour! And here a file can be deleted or renamed during it is still opened. And a file can be opened several times (for reading and writing).	CODESYS Control
CDS-64663	**WebServer:** Specific directory traversal access possible	**[[GENERAL]]** For more details see Advisory 2019-01, which is available on the CODESYS website: https://customers.CODESYS.com/fileadmin/data/customers/security/2019/Advisory2019-01_CDS-64543.pdf	CODESYS Control
CDS-64867	**CmpSettings:** Not allowed character in SetStringValue	**[[COMPATIBILITY_INFORMATION]]** Settings in the CODESYSControl.cfg File: From now on "=" characters are allowed in the values of settings of the type string. The first "=" character in a line is the delimiter between the key and the value.	CODESYS Control
CDS-65080	**CmpOPCUAServer:** Crash if invalid request is sent	**[[GENERAL]]** For more details see Advisory 2019-07, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-07_CDS-65080.pdf	CoDeSys Control
CDS-65149	**CODESYS Control:** Possible DoS vulnerability of communication servers	**[[GENERAL]]** For more details see Advisory 2019-06, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-06_CDS-65149.pdf	CoDeSys Control
CDS-65459	**CmpEventMgr:** Reentrant calls of the same callback from different task contexts not possible	**[[COMPATIBILITY_INFORMATION-OEM]]** Callback functions registered for events are now called concurrently. That means that if a callback function registered for an event is currently being executed and the event is triggered again, then the callback function will be called again concurrently. Therefore, the developer of a callback function is now responsible for making its implementation reentrant. In addition, the developer of a callback	CODESYS Control

		function is responsible for avoiding recursive triggering of the event within its registered callback function. **[[COMPATIBILITY_INFORMATION-EndUser]]** Callback functions registered for events are now called concurrently. That means that if a callback function registered for an event is currently being executed and the event is triggered again, then the callback function will be called again concurrently. Therefore, the developer of a callback function is now responsible for making its implementation reentrant. In addition, the developer of a callback function is responsible for avoiding recursive triggering of the event within its registered callback function.	
CDS-65847	Incorrect permission inheritance for file system objects	**[[GENERAL]]** For more details see Advisory 2019-04, which is available on the CODESYS website: https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-04_CDS-65847.pdf Was already fixed by CDS-58163 for version V3.5.13.0 and now newly assessed.	CoDeSys Control
CDS-66221	**CmpLog:** Support of logger timestamps in console and file in ISO8601 format	**[[COMPATIBILITY_INFORMATION]]** The timestamp of the logger is now changed in the console windows and the logfiles to ISO8601 format: Format: YYYY-MM-DDThh:mm:ss.mmmZ - YYYY=year - MM=month - DD=day - T=delimiter - hh=hour - mm=minutes - ss=seconds - mmm: milliseconds - Z=zulu time / UTC	CODESYS Control
CDS-66341	**VxWorks:** Add -std=c99 compiler setting to VxWorks GNU builds	**[[COMPATIBILITY_INFORMATION-OEM]]** The previously used ANSI / C89 C standard GNU compiler option for building the CODESYS control runtime for WindRiver VxWorks has been adjusted to	CoDeSys Control

		support now C99 C standard extensions in the CODESYS control runtime C/C++ sources. (For further information about ANSI C99 support please refer to the CODESYS Control V3 Manual - Chapter Coding Guidelines)	
CDS-67157	**WinCE:** Huge Cycle Time deviation when calling LogAdd.	**[[COMPATIBILITY_INFORMATION-OEM]]** From Version 3.5. SP15, the Windows CE runtime system has changed its default behaviour regarding logging. Now logger messages are dumped (written to files) asychronouosly, in older versions they were dumped immediately. This behaviour can be overwritten through the CODESYSControl.cfg file option: [CmpLog] Logger.nnn.Type=0x2404 (the bit with value 0x0400 must be set for dumping immediately) Reading the comments regarding logger options in the Windows CE template configuration file in the runtime system deliveries is strongly recommended! For normal production, systems should be configured with dumping asychronously, and the file backend should also be deactivated. **[[COMPATIBILITY_INFORMATION-EndUser]]** From Version 3.5 SP15, the Windows CE runtime system has changed its default behaviour regarding logging. Now logger messages are dumped (written to files) asychronouosly, in older versions they were dumped immediately. This behaviour can be overwritten through the CODESYSControl.cfg file option: [CmpLog] Logger.nnn.Type=0x2404 (the bit with value 0x0400 must be set for dumping immediately) If possible, have a look at the logger options in the Windows CE runtime system configuration file (CODESYSControl.cfg) For normal production, systems should be configured with dumping asychronously, and the file backend should also be deactivated.	CoDeSys Control

CDS-14320	**SysCom:** wrong datatype for bRTSControl and bDtrControl, has to be BYTE	**[[COMPATIBILITY_INFORMATION-OEM]]** The structure COM_SettingsEx has been changed in SysComItf.h! The structure remains binary compatible, but the following 2 parameters are changed: - bDtrControl -> byDtrControl and the type from BOOL -> BYTE - bRtsControl -> byRtsControl and the type from BOOL -> BYTE	CODESYS Control, Libraries
CDS-63686	**Visu, Meter:** Element draws bigger than configured	**[[GENERAL]]** Requires Visu-Profil >= 3.5.15.0 [[COMPATIBILITY_INFORMATION-EndUser]] The size and location of the meter is slightly changed due to a bug in the painting of the element	CODESYS, Libraries
CDS-64208	**Gateway:** Insufficent check of service header	**[[GENERAL]]** For more details see Advisory 2019-03, which is available on the CODESYS website: https://customers.CODESYS.com/fileadmin/data/customers/security/2019/Advisory2019-03_CDS-64208.pdf	Gateway Server
CDS-65123	**Gateway:** GatewaySession could be hijacked	**[[GENERAL]]** For more details see Advisory 2019-02, which is available on the CODESYS website: https://customers.CODESYS.com/fileadmin/data/customers/security/2019/Advisory2019-02_CDS-65123.pdf	Gateway Server
CDS-65124	**Gateway:** Channel number uses insufficiently random values	**[[GENERAL]]** For more details see Advisory 2019-02, which is available on the CODESYS website: https://customers.CODESYS.com/fileadmin/data/customers/security/2019/Advisory2019-02_CDS-65123.pdf	Gateway Server
CDS-21761	**Linux CAA File:** Renaming of files and directories is possible even though they are still opened	**[[COMPATIBILITY_INFORMATION]]** Contrary to the original CAA specification the renaming of files and directories is possible even if they are opened! This behavior is dependent of the underlying operating system and file system.	Libraries
CDS-21762	**Linux CAA File:** Removing of files is possible even though they are still opened	**[[COMPATIBILITY_INFORMATION]]** Contrary to the original CAA specification the deletion of files and directories is possible even if they are opened! This behavior is dependent of the	Libraries

		underlying operating system and file system.	
CDS-69059	**ChannelServer:** Memory allocation DoS	**[[GENERAL]]** For more details see Advisory 2020-01, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=12977&token=33f948eed0c2fd69d238d9515779be337ef7592d&download=	CODESYS Control, Gateway Server
CDS-69600	**VxW7_0620 / LLVM:** Add check for INCLUDE_DATA_NO_EXEC in VxWorks kernel	**[[GENERAL]]** With VxWorks 7 SR0620 the VxWorks Core OS kernel hardening features are enabled by default. One of the hardending features is INCLUDE_DATA_NO_EXEC. With this feature it is not possible to run generated IEC (machine) code from memory of the target. At startup of the VxWorks CODESYS runtime a check for this feature will be performed and if present, the startup of the VxWorks CODESYS runtime will abort.	CODESYS Control
CDS-69665	**CmpRouter/CmpRouterEmbedded:** Crafted packet may cause a DoS	**[[GENERAL]]** For more details see Advisory 2020-02, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13077&token=3bfc6d1d08415a6260b96093520071f5786e7fd4&download=	CODESYS Control
CDS-69672	**Webserver:** Remote heap buffer overflow vulnerability	**[[GENERAL]]** For more details see Advisory 2020-03, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13078&token=de344ca65252463cc581ef144e0c53bd97b8f211&download=	Web Visualization
CDS-69676	**CmpRouter/CmpRouterEmbedded/CmpBlkDrvTcp:** Crafted packets may cause a DoS	**[[GENERAL]]** For more details see Advisory 2020-02, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13077&token=3bfc6d1d08415a6260b96093520071f5786e7fd4&download=	CODESYS Control
CDS-70006	**WinCE:** Reading/Writing 64 bit values to Cortex devices is incorrect	**[[COMPATIBILITY_INFORMATION]]** On Windows Embedded Compact 2013 devices with Cortex CPU, the 64 bit integers are no longer atomically	CODESYS

		accessed. This affects monitoring, and online writing/forcing of values.	

2 Known Limitations

Reboot required to restart a VxWorks PLC

Due to the restriction that the OpenSSL stack can't be re-initialized, it is no more possible to re-start a PLC under VxWorks, if the component CmpOpenSSL is included in the runtime. In such a case, if the PLC has to be re-started, a complete reboot of the hardware is necessary.

3 OEM information from JIRA

To read up on implemented features and changes you can use your JIRA account. Please find some **example** filters below.

List of features and changes:

fixVersion = "V3.5 SP15 Patch 4"

fixVersion = "V3.5 SP15 Patch 4" AND issuetype = "New Feature"

List of features and changes since CODESYS V3.5 SP15:

fixVersion IN ("V3.5 SP15 Patch 4", "V3.5 SP15 Patch 3", "V3.5 SP15 Patch 2", "V3.5 SP15 Patch 1", "V3.5 SP15")

List of issues with compatibility information and known limitations:

fixVersion = "V3.5 SP15 Patch 4" AND (text ~ COMPATIBILITY_INFORMATION OR text ~ KNOWN_LIMITATIONS)

4 History

Created: Sebastian Rothärmel (Quality Assurance)

Reviewed: Bernhard Reiterer (Quality Assurance)

Released: Bernhard Reiterer (Quality Assurance)