Release Note CODESYS V3.5 SP18 Patch 2

03.06.2022

1 Release Notes

Key	Summary	Release Note	Component/s
CDS-81452	CmpBlkDrvTcp: Possible socket blocking DoS vulnerability	**[[GENERAL]]** For more details see Advisory 2022-09, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17128&token=bee4d8a57f19be289d623ec90135493b5f9179e3&download=	CODESYS Control
CDS-81453	Runtime: Possible channel blocking DoS vulnerability	**[[GENERAL]]** For more details see Advisory 2022-09, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17128&token=bee4d8a57f19be289d623ec90135493b5f9179e3&download=	CODESYS Control
CDS-81306	OPC Server: Secure password used for PLC login	**[[GENERAL]]** For more details see Advisory 2022-10, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17129&token=1c1485c4a700c04f2069699f5be7558d276ca117&download= **[[COMPATIBILITY_INFORMATION]]** See manual of the CODESYS OPC DA Server, section OPC Config Tool, to learn more about compatibility and restrictions.	OPC Server, PLC Handler
CDS-56565	UTF-8 Encoding for STRINGs	**[[GENERAL]]** There is now a compiler option to change the encoding of the data type STRING. With the option checked, a STRING will be interpreted as encoded in UTF-8. I.e. any	CODESYS

		STRING literal 'asdf' will be encoded in UTF-8. Monitoring of STRING will decode STRING-values from UTF-8. Alternatively it is possible to mark only specific string literals as UTF-8. This is accompanied by new monitoring attributes to have a strings content monitored as UTF-8 explicitly. The Static Analysis Light and the compiler also have additional checks and rules for detecting cases where the new UTF-8 option should be enabled. They also have new checks for strings operations which might only work on ASCII strings but not on UTF-8 strings anymore.	
CDS-63824	Setup: Uninstallation should delete installation folder	**[[GENERAL]]** New property CDS_DELINSTALLDIR can be set at installation 1=Delete the destination folder INSTALLDIR at uninstall (Default) 0=Do not delete destination folder INSTALLDIR at uninstall If INSTALLDIR is not a subfolder of ProgramFiles or ProgramFiles(x86), INSTALLDIR is not deleted regardless of CDS_DELINSTALLDIR For more information see the documentation "CODESYS Installation OEM Adaptations" and "CODESYS Installation Extended OEM Adaptions"	CODESYS
CDS-65416	AP-UserManagement: Group derivation does not work	**[[GENERAL]]** As the "group in group" concept was removed from the runtime with CDS-65415, the possibility to configure having a group within a group was also removed from the IDE. So now a group will only contain users as members.	CODESYS
CDS-71854	Package Manager: Check Dependencies always	**[[GENERAL]]** Dependencies (MinimumPlugin, MaximumPlugin or MinimumProfile) will now be evaluated independently from the package's content. In previous version	CODESYS

		these depenencies were only be checked if there is a profile relevant content include (ProfileChange, AddMenuConfiguration, AddToolBarConfiguration,...). **[[COMPATIBILITY_INFORMATION]]** If these dependencies has been used without any profile relevant content the installation will fail now.	
CDS-77156	BinaryFormatter: Vulnerability caused by deserialization of untrusted culture settings	**[[GENERAL]]** For more details see Advisory 2021-13, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c498941d9fda86490bca98ff21928eec08a&download=	CODESYS
CDS-77163	AccessDenied exceptions during setup or CODESYS startup	**[[GENERAL]]** ShadowCopy was deactivated for the executables CODESYS, PackageManager, PackageManagerCLI and IPMCLI Every call to one of this executables will result in a selfcall to the same executable, in which the called function is executed. In the wrapping call all files which need to be copied are copied after the inner call finished execution. If an error occurs during the copy operations a rollback is performed. If this rollback is not possible or fails, the installation will be marked as corrupted and a reinstall will be required. **[[COMPATIBILITY_INFORMATION-OEM]]** Having removed the .Net Shadow Copy mechnism may lead to access denied exceptions within OEM code trying to overwrite assemblies that are currently loaded. This may occur with OEM plugins running in a standard CODESYS executable during installation of plugins or packages via Autmation Platform API. Not affected are custom OEM executables still having .Net Shadow Copy active and installations via PackageManager or IPM executables.	CODESYS
CDS-77324	Compiler, Download: Erroneous behavior after	**[[GENERAL]]** Compiler Version >= 3.5.18.0	CODESYS

	download regarding variable values	The compiler calculates the result of constant expressions during compile time. The fix may lead to different calculations, and this can lead to a different behavior of the application. Especially in cases, where intermediate results of the calculation exceed the type Range of some of the constants in the expression. The Compiler now calculates the expression as LINT-expression or ULINT-expression and casts the result as used in the expression. In this case a complex expression is evaluated the result is cast to LINT and assigned to an LINT.	
CDS-77359	BinaryFormatter: Vulnerability caused by deserialization of untrusted profile data	**[[GENERAL]]** For more details see Advisory 2021-13, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c498941d9fda86490bca98ff21928eec08a&download=	CODESYS
CDS-77364	BinaryFormatter: Vulnerability caused by deserialization of untrusted data in the package management	**[[GENERAL]]** For more details see Advisory 2021-13, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c498941d9fda86490bca98ff21928eec08a&download=	CODESYS
CDS-77365	BinaryFormatter: Vulnerability caused by deserialization of untrusted "MissingTypes" data	**[[GENERAL]]** For more details see Advisory 2021-13, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c498941d9fda86490bca98ff21928eec08a&download=	CODESYS
CDS-78280	Menu PackageManager should be replaced by Installer	**[[GENERAL]]** If an CODESYS Installer with a version equal or higher than 1.2.0 is installed, the menu entry Tools -> PackageManager... is replaced with Tools -> CODESYS Installer... Instead of the PackageManager this new entry will open the CODESYS Installer to manage the packages of the current installation. A new Customization Hook was	CODESYS

		introduced ("PackageManagement", "DoNotUseInstaller"), if set to true the PackageManager entry will be used even if the CODESYS Installer is installed in a version higher or equal to 1.2.0	
CDS-78571	Package import from previous installation breaks package signature	**[[GENERAL]]** Packages have been removed from the import assistent. Packages can be easily installed via CODESYS Installer. Furthermore required Packages (Add-ons) will be checked during project analysis during project load.	CODESYS
CDS-79032	ProjectSource: Creating a new project as library will result in a project	**[[COMPATIBILITY_INFORMATION-OEM]]** The methods Engine.CreateProject() always change the file extension always to ".project" but now it only does it if the file extension is different to ".library".	CODESYS
CDS-80861	Project open is not possible on Win8.1 32bit	**[[GENERAL]]** Since the market share of Windows 8.1 is relatively small and a simple fix exists, the issue is not resolved. Installing .Net Framework 4.7.2 or 4.8 will fix this issue.	CODESYS
CDS-31565	CmpDevice: Multisession management needed	**[[COMPATIBILITY_INFORMATION-OEM]]** The CODESYS Control runtime now supports more than one session on a channel. This allows the CODESYS Webvisu to authenticate multiple sessions independently on a single communication channel. As a result, there is no longer a strict 1:1 mapping between session and communication channel in the CODESYS protocol. Accordingly, the functions DevGetSessionId() and ServerGetSessionId(), which provided the associated session for a channel, can no longer be implemented in a meaningful way and have therefore been removed completely. At the same time, new events were	CODESYS Control

		introduced with CDS-71596 to be informed about significant changes to a session. These are signaled between the existing OpenChannel and CloseChannel events: EVT_DevSBeforeCreateSession EVT_DevSSessionDeleted Since the DevGetSessionId() and ServerGetSessionId() functions were used to retrieve the associated SessionID in the event EVT_ChSChannelClosed, the event EVT_DevSSessionDeleted can simply be used here instead to get the SessionID directly as an event parameter. With other words, the EVT_DevSSessionDeleted replaces the previous combination of EVT_ChSChannelClosed and the extra call of DevGetSessionId()/ServerGetSessionId(). In addition, the following functions were incompatibly adapted and thereby removed from the interface of the CmpIecVarAccess component, as they were intended for internal call only: IecVarAccCreateVarList() IecVarAccDeleteVarList() IecVarAccDeleteVarLists() IecVarAccDeleteAllLists() IecVarAccVarListGetFlags() IecVarAccAppendVar() IecVarAccRemoveVar() IecVarAccGetFirstVar() IecVarAccGetNextVar() IecVarAccInvalidateVar()	
CDS-65415	UserMgr: Group derivation for rights check does not work	**[[GENERAL]]** As the group in group was never	CODESYS Control

		evaluated by the runtime system this relationship has been removed. Configuration and checking access rights is not easy and strait forward when access rights are derived from on group to another. This removed relation ship has no effect on effective access rights.	
CDS-74959	VxWorks: OPCUA port 4840 down on stress test (TCP) on another port	**[[GENERAL]]** For more details see Advisory 2021-10, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14806&token=637e12e86301b83beac1653bd88da3aa5aa3f51b&download=	CODESYS Control
CDS-75073	RTS configuration file can be modified by malicous IEC code	**[[GENERAL]]** For more details see Advisory 2022-02, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17089&token=cc5041e24fc744a397a6f6e3b78200a40e6fcd53&download= **[[COMPATIBILITY_INFORMATION]]** CODESYS Control runtime configuration files can no longer be accessed through CAA File, SysFile, SysFileAsync, or other file access libraries.	CODESYS Control
CDS-75246	WebServer: The server should not return the content of all files	**[[GENERAL]]** For more details see Advisory 2021-11, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16803&token=0b8edf9276dc39ee52f43026c415c5b38085d90a&download=	CODESYS Control
CDS-75308	CmpHilscherCIFX / Profinet / Redundancy: Sporadic bus failure switching redundant plcs	**[[COMPATIBILITY_INFORMATION-OEM]]** The following events are renamed because of compatibility problems with 3.5.17.0 CIFX drivers: EVT_ID_CMP_PACKET_INDICATION2 => EVT_ID_CMP_PACKET_INDICATION3	CODESYS Control

		EVT_ID_CMP_PACKET_CONFIRMATION2 => EVT_ID_CMP_PACKET_CONFIRMATION3	
CDS-75358	Crash in CmpSettingsSrv when parsing crafted request	**[[GENERAL]]** For more details see Advisory 2022-06, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	CODESYS Control
CDS-76136	VxWorks: OPCUA port 4840 down on max. concurrent connection scan	**[[GENERAL]]** For more details see Advisory 2021-10, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14806&token=637e12e86301b83beac1653bd88da3aa5aa3f51b&download=	CODESYS Control
CDS-76140	Web server crashes when subjected to HTTP header memory exhaustion attack	**[[GENERAL]]** For more details see Advisory 2021-09, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14805&token=f0b86f99bb302ddd4aadec483aed5f5d3fddbf1a&download=	CODESYS Control
CDS-76491	BACnet: CmpBACnet - BACnetOpenClientCustomer wrong return type	**[[COMPATIBILITY_INFORMATION]]** FUNCTION BACnetOpenClientCustomer wrong return type was changed to IEC_BACNET_HANDLE.	CODESYS Control
CDS-76651	VxWorks: Implement SysSockGetFirstAdapterInfo to support gateway address	**[[GENERAL]]** Ethernet Adapters may have several default routes. Only first route is displayed. Functionality to read route information of an Ethernet adapter is only supported for VxWorks7 and newer versions.	CODESYS Control
CDS-77172	SysDrv3S.sys: Local privilege escalation to system level	**[[GENERAL]]** For more details see Advisory 2022-03, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17090&token=6cd08b169916366df31388d2e7ba58e7bce93508&download=	CODESYS Control

		To make the fix effective, you have to update the SysDrv3S.sys driver to latest V3.5.18.0 manually: - In the Microsoft Windows Device Manager right-click on the Hilscher device to open the context menu. - Select Update driver within this. - Install the driver from the subdirectory "./Driver" of your CODESYS Development System V3 or CODESYS Control installation directory. - Check the driver version after the update. The driver must have version number 3.5.18.0. **[[COMPATIBILITY_INFORMATION-EndUser]]** The SysDrv3S.sys V3.5.18.0 supports the Hilscher PC fieldbus cards only. Thus, the following hardware can no longer be used with the SysDrv3S.sys driver: - "SysDrv3S Automata CAN PCI 2N" = SysDrv3S, PCI\VEN_10B5&DEV_9050&SUBSYS_34551971” - "SysDrv3S Peak PCAN-PCI" = SysDrv3S, PCI\VEN_001C&DEV_0001&SUBSYS_0004001C” - "SysDrv3S Peak PCAN-EXPRESS" = SysDrv3S, PCI\VEN_001C&DEV_0003&SUBSYS_0002001C” Please contact the CODESYS support if you need to use this driver with one of the PC fieldbus cards listed above or any other currently unsupported hardware.	

CDS-78510	Runtime generates weak ChannelIDs	**[[GENERAL]]** For more details see Advisory 2022-04, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17091&token=c450f8bbbd838c647d102f359356386c6ea5aeca&download= **[[COMPATIBILITY_INFORMATION-OEM]]** The obsolete marked function NetServerGetChannelInfoByIndex() was removed completely, use NetServerGetChannelInfoByIndex3() instead. The interface between the CmpChannelClient, CmpChannelServer/CmpChannelServerEmbedded, CmpChannelMgr/CmpChannelMgrEmbedded components was reworked, especially the L4 packet processing structures were redesigned.	CODESYS Control
CDS-78845	CmpUserMgr: anonymous login is still allowed after anonymous login is deactivated	**[[GENERAL]]** For more details see Advisory 2022-05, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17092&token=a556b1695843bb42084dc63d5bdf553ca02ea393&download=	CODESYS Control
CDS-78898	CmpUserMgr: Relogin should support changing account	**[[COMPATIBILITY_INFORMATION]]** The behavior of UserMgrRelogin was extended. This function now allows to switch to another user account. If this is allowed by a session and the session builds up a cache of usernames or access rights itself (instead of using the UserMgr cache) this cache has to be cleaned up.	CODESYS Control
CDS-79100	[Remove Product from Setup] [Product discontinuation] Windows CE 5	**[[GENERAL]]** Win CE5 files are no longer part of PLCHandler SDK.	CODESYS Control
CDS-79444	CmpTraceMgr: Denial of Service vulnerability	**[[GENERAL]]** For more details see Advisory 2022-06,	CODESYS Control

		which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&download=	
CDS-79805	update BACstack to V15.0.1.1	**[[GENERAL]]** BACstack updated to V15 to support BACnet protocol revision 15. **[[COMPATIBILITY_INFORMATION]]** BACnet protocol revision 15 forced some API (DUT) extension, most notably BACNET_ENGINEERING_UNITS and IEC_BACNET_STACK_CONTROL_TYPE . CmpBACnet provides compatibility to protocol revision 14 behaviour by mean of setting/keeping Device.Protocol_Revision to 14. BACnet protocol revision 15 behaviour is enabled by setting Device.Protocol_Revision to 15.	CODESYS Control
CDS-80231	Webserver: Possible crash due to out of bounds read	**[[GENERAL]]** For more details see Advisory 2022-07, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17094&token=2fb188e2213c74194e81ba61ff99f1c68602ba4d&download=	CODESYS Control
CDS-77170	Gateway: DOS due to null pointer dereference	**[[GENERAL]]** For more details see Advisory 2021-12, which is available on the CODESYS website: https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16804&token=d8c89c887979b22fdfc9fd5c3aa3804bbb1ddbff&download=	Gateway Server

2 Known Limitations

PPC VLE

The VLE variant of the PPC compiler could not be tested for this release. Therefore, we discourage the use of the 3.5.18.0 PPC compiler on VLE platforms.

Runtime VxWorks C++

The C++ implementation of the VxWorks runtime is not available for 3.5.18.0. Certain calls to the runtime from the IEC-Application may lead to runtime exceptions. For details see https://jira-intern.codesys.com/browse/CDS-81167.

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 IN ("V3.5 SP18 Patch 1", "V3.5 SP18 Patch 2")

fixVersion IN ("V3.5 SP18 Patch 1", "V3.5 SP18 Patch 2") AND issuetype = "New Feature"

List of features and changes since CODESYS V3.5 SP18:

fixVersion IN ("V3.5 SP18", "V3.5 SP18 Patch 1", "V3.5 SP18 Patch 2")

List of issues with compatibility information and known limitations:

fixVersion IN ("V3.5 SP18 Patch 1", "V3.5 SP18 Patch 2") AND (text ~ COMPATIBILITY_INFORMATION OR text ~ KNOWN_LIMITATIONS)

4 History

Created:	Markus Brüchle (Quality Assurance)
Reviewed:	Bernhard Reiterer (Quality Assurance)
Released:	Bernhard Reiterer (Quality Assurance)