Premium Copro Firmware History

TSXP574634, TSXP575634, TSXP576634

Version #	Date of Publication	Internal reference	Description
SV6.1	**1/2020**	PEP0555453R	Resolved and issue where retransmissions caused a delay in the communications. The retransmissions were caused due to the Master cycle time being greater than the IO Scanner 'Rep rate'. The code was modified to drop the retransmission packets.
		PEP0557748R	Resolved a reboot vulnerability with an HTP script.
		PEP0557749R	Resolved a vulnerability where a Stack Buffer Overflow results in a crash.
		PEP0557750R	Resolved an unauthenticated Reflected XSS (Cross-site scripting) vulnerability.
		PEP0557769R	Resolved an unauthenticated HTTP Password Reset to Default
		PEP0557767R	Resolved a Password change vulnerability to CSRF (Cross-site Request Forgery)
		PEP0557768R	Resolved an unauthenticated HTTP Password Change
		PEP0540655R	Resolved a vulnerability to obtain information on an SMTP server configuration, including registration data of the user.
SV6.0	**11/2018**	PEP0425771R	Resolved an IO scanning communication issue between the CPU Copro and PRM (TCSEGPA23F14F) Profibus Gateway module.
SV5.8	**4/2016**	PEP0318880R	Removed a Remote Code Execution vulnerability in the websSecurityHandler (Advisory ICSA-15-351-01)
		PEP0318881R	Removed a web server vulnerability to a remote file inclusion attack. (ICS-ALERT-15-224-02)
SV5.7	**4/2015**	PEP0283645R	Resolved an issue where Global Data did not always start after a power cycle or Hot Standby switchover. Global Data's initialization was not completing before the Device Manager sent the next command. Now, the device manager will not send a new command until it is notified that Global Data task initialization is complete.
		PEP0277388R	Web pages now meet requirements to work with Java version 1.8.
		PEP0275523R	Data Editor web page functionality is misleading and implies that unlocated symbols can be used. Only modules that are FactoryCast capable can use symbols in the Data Editor web page. The apparent use of symbols was removed from the web pages of non-FactoryCast modules.
SV5.6	**10/2014**	PEP0271979R	Resolved an issue where the I/O Scanner communications could take at least 40 seconds or more to recover if a link down/up event occurs on the client (Copro) side of the switch. A link down/up event (without a duplicate IP on the network) will restart the I/O Scanner in 2-3 seconds.
SV5.5	**6/2014**	PEP0241427R	Resolved Cyber Security vulnerabilities with FTP and HTTP with option added to prevent FTP/HTTP access.
		PEP0250560R	Removed a vulnerability in HTTP, using directory traversals, an attacker could bypass the basic authentication mechanism. (Advisory ICSA-14-273-01)
		PEP0251116R	The Java dialog box displayed a warning indicating an unsigned application. Web page files with Java Version 1.7 now have security Signature.
		PEP0244126R	Resolved an issue where under some rare Modbus TCP traffic and CPU backplane timing conditions, some Modbus responses are matched with the wrong query.
SV5.2	**12/2013**		Resolved an issue where the online display of the TSXIBY100 debug screen was slow or nearly impossible to view the correct data values.

SV5.1	**10/2013**		MIB and MIG agents were corrected to resolve SNMP webFailedAttempsts(1.3.6.1.4.1.3833.1.5.4) and webSuccessfulAccess (1.3.6.1.4.1.3833.1.5.4) that did not increment.
SV4.2	**1/2013**		Resolved an issue where the Copro did not handle errors returned from the host interface and would timeout instead. The Comm blocks configured to the COPRO now works as per block specifications, passing errors to the application instead of timing out, unless no response is received within the timeout specified.
			Resolved an issue where using I/O Scanner could cause excessive ARP traffic for a gateway. Each line of an I/O scanner issued its own ARP prior to establishing a connection, resulting in excessive traffic for a router or gateway. Now, the I/O Scanner will issue an ARP for each IP address rather than for each line of the scanner. This will eliminate multiple ARPS to the same device.
SV4.0	**7/2012**		Response to ICS-ALERT-12-020-03. The CoPro is vulnerable to FTP buffer overflows. A problem due to FTP buffer overload was addressed and the vulnerability has been corrected.
SV3.8	**6/2012**		Two copies of FDR .prm files should be created in both RAM and FLASH. The FLASH version of the PRM file was not created. A change to an algorithm corrected the task to create the FLASH version.
			Added Sub-Function code 10 to the SEND_REQ block. The local Ethernet Coprocessor will initiate a warm reboot sequence when it receives a SEND_REQ block command with OpCode 0x37 and SubFunction code 0x10.
			Cyber Security changes: Removed Telnet service. Removed Windriver debug port. Removed unused password access points.
			A request was made to increase the TTL (Time to Live). The TTL was increased to 32.
			Corrected an issue where the Ethernet Copro Exec version on the web pages was wrong.
			Added an option to the I/O Scanner to increase the timeout time when communicating through Gateways. An option was added to the I/O Scanner in Unity v7.0 and higher where the user can change the retry and retransmission rate when communication with gateways. Slower responding devices (Gateways) can cause a problem in communications.
SV3.7	**12/2011**		Special Note: Premium Copro's at **PV25** integrate a new hardware component only compatible with exec versions 3.3 and higher. These Copro's cannot be downgraded to Exec versions less than 3.3
			Under some conditions, Unity 6 will return an error after an Ethernet download. The handling of new downloaded configurations in the device have been resolved to prevent Unity Pro TCP disconnections when updating the controller through the Ethernet module IP address.
			I/O scanner operation does not always trigger fast retransmission behavior in various devices. The I/O Scanner stack does not implement a series of "3" Keep-Alive ACKs to prompt most remote devices of a lost response packet after receiving the initial ACK from the remote for the Modbus Query I/O Scanner sent. Keep-Alive ACKs from the I/O Scanner stack were increased to "3" from where it is now to be more standard and close to other devices.
			Repeated access to the diagnostic statistics web page causes web server connection to break. Repeated rapid access or refreshing of the Diagnostic Statistics web page can cause the web server to lose its connection. Corrected a race condition that led to an endless loop.
			I/O Scanner would not support a specific combination of Rep Rate and Health Timeout. The combination of a 30ms repetition rate and 50ms Health Timeout leads to triggering Health Timeout in less than 50ms. This is due to a slight delay in the CPU while it is handling FDR synchronization. The priority of the task controlling the Health timeout was raised eliminating the problem.

SV3.5	**6/2011**		Updated Rack Viewer Web page V5.0. Redesigned web pages using Microsoft SilverLight and new features added: • Faster page update times than the traditional FactoryCast web pages that use JAVA. • Pan and Zoom in the Rack Viewer to see a particular drop or module. • New Rack Viewer will allow for a "System View" where Remote I/O is included in the view (ERIO, RIO and MB+ DIO for Quantum) • An option is provided in Unity Pro 6.0 to disable the SilverLight Rack Viewer pages to save memory in the PLC. The legacy Rack Viewer pages will be used instead. • It will no longer be necessary to re-import the Unity program into Web Designer and download to the module after a program change.
			CoPro Reboots after Cable Break with Explicit Messaging. In some instances, the Copro reboots while Explicit messages are configured to devices that do not exist and a link loss event occurs at the Copro. The connection table management was improved.
SV3.3	**12/2010**		I/O scanner not scanning at configured rep-rate. The I/O Scanner may not operate at the configured Rep Rate if its configured rate is greater than 1 second. If the Rep Rate is configured for a value of 5 msec, the actual rep rate will vary between 1ms and the configured rate of 5 msec. Modified I/O Scanner task priorities.
			I/O scanner health bits will not return to healthy state (1) after a TesysPort is power cycled. Sometimes after power cycling a TesysPort, the respective I/O Scanner health bits in the CoPro changes to a state value of zero (0) and never changes back to a value of one (1) after power is re-applied to the TesysPort.
			Copro does not send a bootp request after it is powered on. The CoPro, with either version 2.5 or v2.7 Exec firmware, does not send a Bootp request after it is powered on if the new PLC was placed on the rack right out of the box with no configuration. Exec firmware version 2.1 did not experience this issue. Modified the firmware to send Bootp requests at power on. Requests are now sent every 5 seconds for 2 minutes.
			I/O Scanner will not open a connection if the device being scanned has a slow response time (110-120ms). Fixed the Retransmission Timeout (RTO) algorithm.
			CoPro port unable to make connection through a router. Any client/server communications to the CoPro outside of the local subnet, could fail in some cases. The Round Trip time algorithm for retransmission was modified.
SV3.1	**5/2010**		Premium CoPro stops I/O scanner communication with slow responding devices. I/O Scanning to devices with varying response times may stop if it receives a reset (RST) from the device. A fix was implemented so that when the Quantum CoPro receives a RST from the server on an established connection, it closes the existing connection and tries to establish a new connection on a different port.
			Premium CoPro can take up to 25 seconds to close a connection. The Quantum CoPro sends a set of six ACKS or Keep-alives followed by a RST. This can take up to 25 seconds before the connection is closed and allowing a new one to open. The code was modified to cancel the retransmit timer.