BMENOC03x1 Firmware History

BMENOC0301 and BMENOC0311

Version #	Date of Publication	Internal reference	Description
SV2.17	**11/2019**	PEP0546763R	Wind River VxWorks TCP/IP stack vulnerabilities. These vulnerabilities had the potential to trigger remote code execution and denial of service conditions. Reference SESB-2019-214-01 for further detail.
		PEP0516084R	Resolved a Windows 10 issue with communications from an application (e.g., OFS) to an eNOC when configured with IPSec. The solution requires: 1. eNOC FW version 2.17 or higher 2. Microsoft update-KB4520062 for Windows 10, 1809 version only. Microsoft is scheduled to release updates in the first quarter of 2020 for Windows 10 versions 1903, 1803, and 1709. https://www.catalog.update.microsoft.com/Search.aspx?q=KB4520062
		PEP0520525R	Resolved an issue connecting to the eNOC web page in a Standby system. This occurred after performing a 'Build All' and download project to the primary PLC, then transferring the program to the Standby PLC.
		PEP0539129R	Resolved slow reconnect issues to the new primary if a switchover occurred on an M580 HSBY and IPsec was configured. The issue could occur after a switchover due to a power cycle on the primary CPU or a command in the program.
		PEP0544289R	Resolved NTP clock time issues if the eNOC was configured as an NTP client and the communications link was configured for IPsec. The issue did not occur if IPsec was not configured.
		PEP0496205R	Resolved an issue where the web page 'Program Viewer' did not work in Unity Pro V13.1.
		PEP0513705R	Resolved an issue when using the web page showing the PLC application, the application sections did not appear.
		PEP0542100R	Resolved an issue where the 'Program Viewer' web page times out if there is an instruction SWAP_ARINT in the Structured Text section.
SV2.16	**4/2019**	PEP0504840R	Corrected a 'Buffer Overflow' vulnerability in FTP Service.
		PEP0524730R	Corrected an Implicit write message byte swap issue that could occur under specific conditions.
		PEP0500118R	Removed the BMENOC firmware version number from being displayed in the Control Expert Debug screen due to a limitation in the display field. The modules firmware version number is displayed correctly in Unity Loader, BMENOC web page, DTM and BMENOC DDT.

PV	**4/2019**	PEP0439906R PEP0218116E	Hardware component changes were made to BMENOC03x1 modules. Due to this change, firmware was also modified for compatibility purposes, resulting in a minimum firmware version (SV) requirement for these modules. The hardware change is identified by a specific PV number on the module. • If the BMENOC0301 PV is greater than or equal to PV13, then the *minimum* firmware version that can be installed is 2.15. • If the BMENOC0301C PV is greater than or equal to PV13, then the *minimum* firmware version that can be installed is 2.15. • If the BMENOC0311 PV is greater than or equal to PV14, then the *minimum* firmware version that can be installed is 2.15. • If the BMENOC0311C PV is greater than or equal to PV14, then the *minimum* firmware version that can be installed is 2.15. Although the new hardware will allow firmware version's less than 2.15 to be installed, it is not recommended as the backplane port will be disabled, regardless of how the backplane port is configured. Re-installing a firmware version of 2.15 or higher will allow the user to 'enable' or 'disable' backplane access.
SV2.15 **IR10** **Web V3.0**	**12/2018**	PEP0483756R PEP0488727R	Corrected an issue where the first RSTP frame sent by the NOC at power up contained the wrong priority value from what it was configured to be.
		PEP0444359R	An option is available to avoid creating an unintentional Ethernet loop caused by connection to the NOC Service Port on a Standby system. To implement this option, select the *Automatic blocking of service port on Standby NOC* check box that appears in the 'Service Port' tab of the configuration dialog. This check box is only available in Control Expert V14 or later. This feature is available in a Hot Standby system using a CPU with firmware V2.8 or later and a BMENOC0301.4 or later module.
		PEP0486375R	Corrected a communication dropout issue between the NOC and an EGX150 Ethernet to Serial Gateway. A specific timing issue occurred which resulted in a 16 second communications outage with the Gateway.
		PEP0490950R	Support for 128 devices/connections. Requires DTM supplied in Control Expert V14. Previously, the NOC could configure 128 Modbus connections but could only configure 112 EIP connections because of the 12 Local slaves.
			As there is limited support for Java and Silverlight in modern web browsers, the modules webpages have adapted to HTML5. Any applications created in Web Designer (custom web pages and graphic editor) will continue to use Silverlight. This change only applies to the BMENOC0311 web pages.
SV2.15 **IR04** Limited Release	**9/2018**	PEP0405262R	Corrected a web page display issue that showed DHCP was enabled even if it was disabled. Functionally, DHCP was disabled but the status was incorrectly displayed in the web page.
		PEP0450964R	Corrected an IO Scanner ARP rate increase after a DIO cable disconnect
		PEP0436072R	Corrected an issue where the BMENOC03x1 web page in a standby system is not accessible after a build all and transfer of the application to PLC's A & B.
		PEP0475432R PEP0465836R	Corrected an issue where the BMENOC3x1 on the HSBY was assigned the MAC derived IP address when the application is transferred from the primary to the standby by the DDT.
		PEP0440826R	Corrected a Buffer overflow vulnerability in the SMTP server.
		PEP0440846R	Corrected a Buffer overflow vulnerability in the Modbus Protocol Parser.
		PEP0440867R	Implemented more robust Memory Management Command code.
		PEP0441166R	Implemented more robust function calls to reduce vulnerabilities of non-secure functions in SDL (MS-Secure Development Lifecycle).
		PEP0441106R	Implemented a more robust 'strncpy' function in code.
		PEP0483756R	Corrected a wrong RSTP priority value when powered on.

SV2.14	**7/2018**	PEP0434047R PEP0439151R	Corrected an issue where some IO Scanning lines stop scanning with bad health status if the server device is power cycled when communicating thru a router. Code changes were implemented to prevent corrupted events in tasks from occurring when the server device was power cycled.
		PEP0447400R	Corrected an issue where the BMENOC03x1, when used as a Modbus server, will respond with wrong values in Modbus registers if the Ethernet cable is disconnected then reconnected while communications are active.
		PEP0414972R	Corrected an issue where the BMENOC03x1, when configured as an address server, might not serve IP addresses to every device located on a different subnet due to the amount of ARP traffic generated to the gateway. This is resolved by limiting the amount of IO Scanner broadcast traffic from the NOC.
SV2.12	**3/2018**	PEP0433465R	Corrected an issue where a large application could not be downloaded to the CPU through the BMENOC03x1 without faulting.
		PEP0427575R	Removed the usage of the IP A and IP B addressing.
		PEP0408893R	An M580 clock can now be updated from a BMENOC03x1 when it is used as an NTP client. Only one NTP client on the same PLC rack can be configured and is supported using the R_NTPC block. *Requires Unity 13 with HF2 which contains DTM 3.9.10 (*scheduled for mid April 2018 release*)
		PEP0400444R	Documentation changes made to Modicon M580 BMENOC0301/0311 Ethernet Communications Module Installation and Configuration Guide, part number HRB62665. A table of Ethernet ports and related 'Services and Addresses' were added to the manual.
		PEP0432956R	A vulnerability has been corrected where a POST HTTP request with very large numbers would cause a crash of the web server.
		PEP0344196R	BMENOC03x1 can now be configured as a Bootp/DHCP client allowing an IP address to be assigned from a remote Bootp/DHCP server. Supported in standalone PLCs only. Not supported in Hot Standby systems. *Requires Unity 13 with HF2 which contains DTM 3.9.10 (*scheduled for mid April 2018 release*)
		PEP0417240R	Corrected an issue where the port could lock up if connected to a hub that is power cycled numerous times (>100). This may occur only if any one of the ports are disabled. It does not occur if all ports are enabled.
		PEP0344198R PEP0414972R	Support was added for slow gateway/bridge devices when using Modbus IO Scanner. A checkbox was added in the DTM Modbus IO Scanner configuration screen 'Request Setting' folder to allow selection for slow responding devices. When the slow gateway option is selected, the firmware increases the number of retransmissions from 3 to 6 at intervals of 1s, 1s, 1s, 1s, 1s, 500ms. *Requires Unity 13 with HF2 which contains DTM 3.9.10 (*scheduled for mid April 2018 release*)
		PEP0427388R	Corrected an issue where some UDP ports remained open despite the service being disabled.
		PEP0433514R	Corrected an issue where the DHCP server stops working after an application was downloaded.
		PEP0428443R	Corrected an issue where the IO Scanner would not establish a connection if a RST, ACK was received after a RST was sent by the NOC when opening an implicit connection.

SV2.11	**12/2017**	PEP0233967E	This firmware version and forward, certifies the modules for CSPN. Certification requires the following: *Note: V2.11 does NOT contain the web updates that support the M580 Safety products as in V2.10. Web support for M580 Safety is restored in V2.12.*
		PEP0384365R	Support for IKEV1 & IKEV2 protocols. CSPN certification requires support for both IKEV1 & IKEV2 protocols. As an IPsec responder, it is required that IPSec connections are allowed to be established with both IKEV1 and IKEV2.
		PEP0384366R	Removing the aggressive mode currently used in IKEV1 protocol.
		PEP0384368R	Use of Diffie Hellman method of 2048 or 1024 bits for cryptographic key exchange (configurable by the user in the DTM)
		PEP0384370R	IPsec implementation of SHA256 instead of SHA1.
		PEP0384371R	IPsec implementation of AES128 instead of 3DES.
		PEP0384372R	IPsec implementation of ESP/confidentiality. (configurable by the user in the DTM)
		PEP0384373R	Requirement for additional complexity in the pre-shared key encryption.
SV2.10	**10/2017**	PEP0241258E	Rack viewer support for the M580 Safety CPU, CoPro, and I/O modules.
		PEP0241258E	PLC Program Viewer and Data Table support for safety variables.
SV2.09	**03/2017**	PEP0352688R	A vulnerability has been corrected where a malformed DHCP packet can cause a CPU exception resulting in unexpected operation.
		PEP0363060R	A vulnerability has been corrected where a module fault may occur with specific malformed IP frames
		PEP0388499R	A fault may occur after receiving a specific rate of PTP (Precision Time Protocol) packets for a period of time.
		PEP0391711R	The output 'ETH_SCE_STATUS', of the Function Block 'ETH_PORT_CTRL', always returns ‘1’ (command is not executed) even though the block is triggered with the right input. The firmware did not check the current state of the service before executing the command and always return a 1 (error) to the ETH_PORT_CTRL control block. A check was added in the firmware to get the current state of the service prior to performing the activation or de-activation of a service and the correct ETH_SCE_STATUS (ETH_PORT_CTRL return status bit in block).
SV2.08	**11/2016**	PEP0296858R	Communication issue with a Rockwell EN2DN. Mismanagement of the Run/Idle bit was resulting in issues establishing communications with some 3rd party products.
		PEP0317270R	Module could end up in a non-working state after a large number of swaps when installed in a Hot Standby system. A fix has been implemented in the RTOS.
		PEP0337251R	Modbus object failure in EIP explicit message. CIP MODBUS requests to class 0x44 returns 0x0C error code. Changes were implemented in the Modbus object handler that resolved the issue.
		PEP0343947R	Now supports a maximum of 64 simultaneous Modbus TCP connections on its server path. Previous versions supported 32 Modbus TCP connections on its server path.
SV2.07	**10/2016**	PEP0341736R	A reboot of the module would occur if the Address server receives a DHCP request from a device that is not in the DHCP server table. For device’s not on the host list, incoming DHCP requests for are now dropped.
		PEP0326354R	Corrected a Diagnostic web page French language issue.

SV2.05	**06/2016**	PEP0314953R	Closing the oldest connection can take up to 1 minute. The new behavior is when the maximum number of Modbus/UMAS server connections is reached, the oldest connection is closed immediately before the new connection is opened.
		PEP0322285R	Corrected an issue where duplicate eNOC IP addresses occurred after a forced M580 HSBY swap.
			Support for 4k word Input/Output.
			Support for IO Scanning through routers.
			Support for DHCP through routers.
SV2.04	**02/2016**	PEP0314029R	Support for M580 Hot Standby functionality.
			Ethernet backplane port is now disabled in no-config for security reason. This had been enabled in no-config in v2.03.
			A_B_IP_ADDRESS_STATUS added in eNOC DDDT. IP Address A/B status (0 in case of duplicate IP or no IP assigned).
			FIRMWARE_VERSION added in eNOC DDDT. Allows CPU WEB RackViewer to display the eNOC firmware version MSB=Major Revision, LSB=Minor Revision
			FDR_USAGE added in eNOC DDDT. % of FDR server usage.
			NETWORK_HEALTH added in eNOC DDDT. 0: A potential network broadcast storm is detected. 1: A network broadcast storm is not detected.
SV2.03	**11/2015**	ART147955	Improved Modbus TCP throughput performance by removing messaging limitations.
SV2.02	**08/2015**	PEP0278967R	It was not possible to deactivate unused Ethernet ports. Deactivation of unused Ethernet ports is now available when used with Unity V10 and the matching Unity V10 DTM.
		PEP0294913R	Deleting a data table from the web page using the delete button on the web page removes the table from the view. But, closing the browser, deleting the history and opening the web page again, the tables remain.
		PEP0295669R	Could not communicate with a Rexorth VT-HNC100. Code modified to allow communications with the Rexorth device where it uses a UDP checksum of 0 in it's CIP IO packets.
SV1.03	**03/2015**		Corrected issues with displaying Web pages.
SV1.01			Initial Release.