BMXNOC0401 Firmware History

Note: *Our firmware are continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:*
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Version #	Date of Publication	Internal reference	Description
SV2.11	**8/22/2022**	PEP0671766R VMT-3979	Resolved a vulnerability that allowed accessing information when a HTTP request is sent to the web server of the device. CVE-2021-22785
		PEP0574466R	Resolved an issue where the NTP time zone did not adjust correctly.
		PEP0671765R VMT-3942	Resolved a vulnerability that could cause denial of HTTP and FTP services when a series of specially crafted requests are sent to the controller. CVE-2020-7549
		PEP1009420R VMT-4087	Resolved a vulnerability that could cause a denial of service when a specially crafted file is sent via FTP. CVE-2020-7563
		PEP0671769R VMT-3985	Resolved a vulnerability that could cause an out of bounds read/write due to specific malformed files.
		PEP0671770R VMT-4089	Resolved a vulnerability that could cause a stack-based buffer overflow due from a repeated file execution.
		PEP1009643R VMT-4169	Resolved an SNMP vulnerability that could result in a Trust Boundary Violation.
		PEP0632772R VMT-2525	Resolved a web file system access vulnerability.
		PEP0671768R VMT-3980	Resolved a vulnerability that could cause denial of service when a specially crafted HTTP request are sent to the web server of the device. CVE-2021-22788
		PEP0671773R VMT-3604,3606	Resolved a vulnerability where accessing unrelated memory locations could result in an out of bounds read.
		PEP0671771R VMT-4091	Resolved a vulnerability where an insufficient Input Validation could cause a denial of service of the device when a specially crafted HTTP request is sent to the web server of the device. CVE-2021-22787
		PEP0655038R VMT-5174	Resolved a weak hashing vulnerability. CVE-2010-2967, CVE-2010-2966
		PEP0675256R VMT-5174	Resolved memory allocation vulnerabilities.
		PEP0636123R VMT-3983	Cybersecurity robustness enhancement by removing a Remote Code Execution vulnerability in web Security Handler. Refer to CVE-2015-6461 for further details.

SV2.10	**2/2020**	PEP0375960R	Resolved a network communications failure when a specific device (Interroll Multicontrol) was powered up on the EIP network.
		PEP0487600R	Corrected an issue where the IO Scanner would not establish a connection if an RST, ACK was received after a RST was sent by the NOC when opening an implicit connection.
		PEP0572850R	Resolved a NOC401 FDR issue where if the Ethernet cable was disconnected for 1 day, it would not respond to DHCP Discovers and TFTP Reads sent by the TesysT when the cable was reconnected.
		PEP0572754R	Resolved a reboot vulnerability with an HTP script.
		PEP0572753R	Resolved a vulnerability where a Stack Buffer Overflow results in a crash
		PEP0572752R	Resolved a vulnerability to obtain information on an SMTP server configuration, including registration data of the user.
		PEP0572643R	Resolved a web server vulnerability that allowed commands to be executed without authentication.
		PEP0572750R	Resolved an unauthenticated Reflected XSS (Cross-site scripting) vulnerability.
		PEP0572749R	Resolved a Password change vulnerability to CSRF (Cross-site Request Forgery)
		PEP0572748R	Resolved an unauthenticated HTTP Password Change
		PEP0572747R	Resolved an unauthenticated HTTP Password Reset to Default
SV2.09	**12/2015**	PEP0309176R	Removed a Remote Code Execution vulnerability in the websSecurityHandler (ICS-VU-587471)
SV2.08	**11/2015**	PEP0306197R	When the BMXNOC0401 is being used as a server and the number of connections requested by the client exceeds 32, the server may return incorrect data on any one of the connections. An issue affecting the Modbus server connection management state machine, has been corrected.
SV2.07	**10/2015**	PEP0268678R	ATV32 did not recognize the BMXNOC0401 as a valid FDR server. Corrected malformed FDR server address sent from the NOC0401.
V1.02	**Bootcode**	PEP0300706R	BMXNOC040X can't be pinged due to MAC address corruption. Under specific set of conditions during power up, the flash memory containing the MAC address became corrupted. Fix prevents MAC address change.
			Removed a web server vulnerability to a remote file inclusion attack. (ICS-ALERT-15-224-02).
SV2.06	**3/2015**	PEP0286599R	If a time returned by an NTP server was earlier than the CPU time, Modbus TCP messages could be lost. The Modbus task was modified to use a tick counter instead of the real-time clock.
SV2.05	**6/2014**	PEP0241427R	Cyber Security vulnerability using FTP or HTTP. Cyber Security - Option added to prevent FTP/HTTP access
		PEP0251116R	Web page issue with Java Version 1.7. Files did not have security signature. The Java dialog box provides a warning indicating that this is a unsigned application. The files all have the proper signature.
SV2.04	**11/2013**		Resolved an incorrect SNMP table information.
			Resolved an SNMP “sysUpTime” issue.
			Added SNMP support for Connexium Network Manager.
SV2.03	**4/2013**		The M340 TOD (Time of Day) clock would reset after a power cycle if a NOC0401 was configured in the system. A TOD reset would occur on a 'Link-up' event on any port on the BMXNOC0401, even though a power cycle was not required. A clock reset was commonly observed after a power cycle of the system.
SV2.02	**1/2013**		An improvement was made to the switch forwarding table. The switch forwarding tables are now flushed on a link down event.
			An improvement was made to the switch driver code. Changes were made to how the driver selects which mode to use to communicate with the Marvel Switch for getting and setting of diagnostic and management data.

SV2.01	**10/2012**		When a part of an RSTP ring made up of the BMXNOC0401 breaks, the ring recovery time can vary depending upon where the break is. Under some conditions the ring does not recover. The state tables were corrected to be consistent. The ring now recovers in the proper manner regardless of where the break occurs.
			Retransmission of a packet requires the issuing of three duplicate ACKs. This is inconsistent with the behavior of other Schneider products and inefficient in an automation environment. The fast retransmission algorithm is now triggered by a single Duplicate ACK.
			The DATA_EXCH block would fault if all links were broken on the NOC0401. When performing this action the order was corrected and when the cable is reconnected an error code will be returned if the device is not ready.
			The recovery time for I/O scanning following a ring break in an RSTP ring takes much longer than the specified time. The retry algorithm for the retransmission time was corrected.
			Various issues related to security were addressed. They include unencrypted passwords, open services that are insecure, multiple well-known passwords and an open debug port in the stack. 1 Encrypted HTTP password file that is stored on file system. 2 Removed Telnet service 3 Removed WindRiver debug port service 4 Use encrypted passwords in the code 5 Removed unused logins/passwords from firmware 6 Recompiled firmware without symbol table
SV1.02	**8/2012**		Communications would halt after approximately 50 days of continuous operation without indication to the user. A power cycle was required to recover communications. The problem was due to the rollover of a set of counters which are used to determine the time of communications.