M340 - BMX P34 1000 / P34 2000 / P34 2010/ P34 20102* / P34 2020 / P34 20302* / P34 2030 firmware history

Schneider Electric

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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
SV3.40	08/2021	PEP0614567R	INT: implementation of a new NAND Flash.
		PEP0621373R	Cybersecurity improvement. For further info please refers to CVE-2021-22785
		PEP0621375R	Cybersecurity improvement. Denial of Service after HTTP and FTP script.
		PEP0621381R	Cybersecurity improvement. Elevation of privilege for webserver after a POST specific script.
		PEP0621384R	Cybersecurity improvement. For further info please refers to CVE-2021-22788
		PEP0633132R	Cybersecurity improvement. For further info please refers to CVE-2021-22786
		PEP0634016R	Cybersecurity improvement. For further info please refers to CVE-2021-22787
		PEP0638097R	Cybersecurity improvement. For further info please refers to CVE-2020-7562
		PEP0638113R	Cybersecurity improvement. For further info please refers to CVE-2020-7564
		PEP0639954R	Cybersecurity improvement. For further info please refers to CVE-2020-7563

Note: Web Pages usage could be limited depending on the types of web browsers used in user's machine.

Please check the FAQ FAQ000219232, available here: https://www.se.com/ww/en/faqs/FAQ000219232/ for further information about compatibility between PLC web server and web browser.

(*) BMXP342010 and BMXP342030 are no more manufactured.

M340 - BMX P34 1000 / P34 2000 / P34 2010/ P34 20102* / P34 2020 / P34 20302* / P34 2030 firmware history

Schneider Electric

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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
SV3.30	10/2020	PEP0543833R/ artf265225	Improvement of cybersecurity: Denial of Service after specific Modbus requests. Reference CVE-2020-7857 for further details.
		PEP0544617R/ VMT-1360	Resolved an unauthenticated HTTP Password Change vulnerability. Reference CVE-2020-7540 for further details.
		PEP0551697R /VMT-1464	Improvement of cybersecurity: Denial of Service caused by a stack buffer overflow. Reference CVE-2020-7539 for further details.
		PEP0581791R /VMT-1257	Improvement of cybersecurity: Information disclosure using a SNMP command. Reference CVE-2020-7541 for further details.
		PEP0582022R	Improvement of cybersecurity: Denial of Service web server making the device non-responsive.
		PE0609172R /VMT–1655	Improvement of cybersecurity: Denial of Service after the possibility to change ARP table through SNMP Reference CVE-2020-7536 for further details.
		PEP0603351R/ / VMT–2525	Improvement of cybersecurity: Elevation of Privilege for webserver after specific HTTP script. Reference CVE-2020-7535 for further details.
		PEP0594007R/ VMT-1705	Improvement of cybersecurity: Denial of Service cause by a specific Modbus command. Reference to CVE-2020-7537 for further details.
		PEP0542676R/ VMT-1545	Improvement of cybersecurity: Denial of Service after HTTP and FTP script. Reference CVE-2020-7549 for further details.
		PEP0516050R/ VMT-1556	Improvement of cybersecurity: Denial of Service after a failed TCP Disconnection. Reference CVE-2003-0001 for further details.
		PEP0548568R/ VMT-1392	Improvement of cybersecurity: Denial of Service, CPU went into an integer overflow managed exception with specific python script. Reference CVE-2020-7542 for further details.
		PEP0578776R/ VMT-1950	Improvement of cybersecurity: Denial of Service, CPU went into a stop managed exception with a specific python script. Reference CVE-2020-7543 for further details
		PEP0609213R/ VMT-3069	Improvement of cybersecurity: Denial of Service, web server allows modifying the URL. Reference CVE-2015-6461 for further details

(*) BMXP342010 and BMXP342030 are no more manufactured.

M340 - BMX P34 1000 / P34 2000 / P34 2010/ P34 20102* / P34 2020 / P34 20302* / P34 2030 firmware history

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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
SV3.30	10/2020	PEP0548481R/ PEP0594618R	Corrected the impossibility to connect to a M340 CPU with a UPro<SV7.0 whatever the SV firmware of the CPU.
		PEP0435109R	Corrected an issue of Modbus over TCP *Write_Var* broadcasting message to a gateway, embedded Ethernet PLC port closed the connection with error after 16 retries.
		PEP0600629R	Corrected of the non-reset of variables in SFC while initializing the SFC.
		PEP0571911R	Resolved BMXAMI0800 input channels randomly set at 0 at PLC power up.
		PEP0550137R	Improved the Card ERR led behavior at the very first start of the CPU.

(*) BMXP342010 and BMXP342030 are no more manufactured.

M340 - BMX P34 1000 / P34 2000 / P34 2010/ P34 20102* / P34 2020 / P34 20302* / P34 2030 firmware history

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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 #	Enhancement		
	OPR/PCR #	bFO Case #	Description
V3.20 (09/19)	PEP0524974R	56289542	Improvement of CAN fieldbus management to prevent the CPU going to Managed Exception state in case of important CAN errors (for example: in case of strong EMC disturbance in the CANbus) .
	PEP0532214R	56916801	Fixes a wrong management of SDO in case of many active MFBs addressed simultaneously without diag check.
	PEP0507205R	INT	Improvement of cyber security protection: robustness in front of Pre-Auth Denial of Service.

(*) BMXP342010 and BMXP342030 are no more manufactured.

Version #	Enhancement		
	OPR/PCR #	bFO Case #	Description
V3.10 (08/19)	PEP0538819R PEP0543481R PEP0523288R PEP0538813R PEP0515690R PEP0543480R	int	Improvement of cyber security protection: Denial of service on invalid inputs
	PEP0538813R		Improvement of cyber security protection: Unauthenticated write data request
	PEP0515686R		Improvement of cyber security protection: Denial of service on invalid application transfer
	PEP0510445R PEP0538810R		Improvement of cyber security protection: Unauthenticated modification of application
	PEP0515686R		Improvement of cyber security protection: Denial of service on PLC reservation
	PEP0538813R		Improvement of cyber security protection: Unauthenticated application transfer N.A. Improves robustness during big amount of project downloads

(*) BMXP342010 and BMXP342030 are no more manufactured.

M340 - BMX P34 1000 / P34 2000 / P34 2010/ P34 20102* / P34 2020 / P34 20302* / P34 2030 firmware history

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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 #	Enhancement		
	OPR/PCR #	**bFO Case #**	**Description**
V3.01 (02/19)	PEP0492242R PEP0492243R	int	Fixes the managed exception error issue in case of private UMAS request sent to CPU.
	PEP0518628R PEP0428256R	int	Enhance cybersecurity and avoid a managed exception error in case of certain communication frames of packets sent to CPU
	PEP0492220R	int	Enhance cybersecurity features regarding Run/Stop input and reservation mechanism management
	PEP0492240R	int	Fixes the managed exception error of CPU if Unity Pro transfer an invalid block.
	PEP0439147R	44108698	Fixes the M340 CPUs stop with managed exception due to HMI Vijeo Designer write to located variables
	PEP0492239R PEP0447659R		Enhance cybersecurity regarding CPU memory robustness
	PEP0503288R		Fixes an halt of pack command. Using a Pack command with a non-consistent application must turn the CPU in HALT, this was not the case before this version, the pack command aborted instead of halted the CPU .
	PEP0501422R		Improves the M340 CPUs firmware allowing to managed a new RS485 transceiver component in CPU.
	PEP0490724R	52336036	Fixes the issue of different behavior between the running of application in simulator and the real target .

(*) BMXP342010 and BMXP342030 are no more manufactured.

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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 Number	OPR or Tempo Number	bFO Case and/or Internal Reference Number	Description
V2.90	PEP0337383R		M340 - To make UMAS server more robust when receiving incorrect UMAS request.
	PEP0335554R		M340 increase of MAST cycle when 2 NOE are configured
	PEP0331130R	26233646	M340 crash during FTP transfer of several hundred files from PLC to FTP client
	PEP0327837R	26233646	M340 crash during FTP transfer of several hundred files from FTP client to PLC
	PEP0297971R	20117728	M340 CPU P342020 (New CPU unused) fails to get NTP time from NOR0200 when first installed

Version Number	OPR or Tempo Number	bFO Case and/or Internal Reference Number	Description
V2.80	PEP0298276R	20154286	If the BMXERT1604 is connected through the BMXNOE0110 with the Testing client in OFS3.5 (SP8), using Data dictionary, the CPU crashes with the Err LED in red.
	PEP0298586R	19685023	**Improvement:** increase the robustness of the serial port to prevent a CPU crash during normal RUN after a misinformed Modbus communication request by connected equipment.
	PEP0310457R		Implementation of the cyber security fix for vulnerability ICS-VU-587471 (GoAhead Web Server

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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

| | | | vulnerability – Schneider Electric communication SEVD-2015-344-01). |

(*) BMXP342010 and BMXP342030 are no more manufactured.

Version Number	OPR or Tempo Number	Vantive Case and/or Internal Reference Number	Description
V2.70	PEP0288243R	UNITY00075931	The IP address configured in the BMXNOC0401 module, when located in the main rack, may be modified by the CPU after a power cycle
	PEP0285449R	UNITY00075374	Enhancement of the password protection function to reserve the PLC.
	PEP0285031R	UNITY00075381	Enhancement to implement the ANYBOOL function on M340
	PEP0276537R	UNITY00075481	Enhancement to allow for the adjustment of the FTP timeout value
	PEP0268402R	UNITY00076086	Enhancement to improve the Real Time Clock robustness and reduce the RTC drift when %S20 is set to 0
	PEP0294104R	UNITY00077794	Bug fix for Quantum DFB icon issue when PCMCIA card is not inserted. Replicated on M340 to maintain Unity Pro consistency.
		UNITY00076143	Bug fix for BMXP342020 where the CPU may crash when read by OFS with the NOE's IP address if the time stamping option is selected
	PEP0277388R		Enhancement for web compatibility with Java 1.8

(*) BMXP342010 and BMXP342030 are no more manufactured.

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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 Number	OPR or Tempo Number	Vantive Case and/or Internal Reference Number	Description
V2.60	PEP0118511R		Quantum cyber security enhancements replicated on the M340 range. A total of 4 enhancements have been completed on M340.
	PEP0246940R		Processor can now restart correctly after a crash
	PEP0256083R		Robustness improvement on Modbus communication request.
	PEP0267656R		Improvement for Ethernet processors about Vxworks issue
	PEP0064074R		Cyber security improvement on M340 CPU web server
	PEP0076557R		Bug fix for Read_SDO
	PEP0190343R		Compatibility with Unity Pro V8 application password protection evolution
	PEP0057845R		Bug fix for "reserved by empty" error message in the reservation process

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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

	PEP0192924R		Cyber security robustness improvement on Webserver

(*) BMXP342010 and BMXP342030 are no more manufactured.

Version Number	OPR or Tempo Number	Vantive Case and/or Internal Reference Number	Description
V2.50	PEP0047851R		Fix Diag Viewer that does not display messages and symbols for instances bigger than 254 in a single section
	PEP0051769R		Enhance timing management for explicit communication EF in case of non responsive slaves
	PEP0060376R		Fix embedded Ethernet port non responsive behaviour after repeated link up/down events
	PEP0056494R		Cyber security enhancements

Version Number	OPR or Tempo Number	Vantive Case and/or Internal Reference Number	Description
V2.40			This version supports LL964 programming language.

Version Number	OPR or Tempo Number	Vantive Case and/or Internal Reference Number	Description

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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 Number			
V2.30	PEP0039565R	1293862	M340 : On SD card file rename issue by FTP
	PEP0038938R	1290591	BMXP342020-Character mode error of the CPU serial port
	PEP0030155R	1214961	bad Canopen telegramm after a write_SDO length <4
		UNITY00047500	Improve performance of data Dictionary Browse requests coming from HMI
	PEP0042677R	1322743	robustness improvement of communication system within the CPU

(*) BMXP342010 and BMXP342030 are no more manufactured.

Version Number	OPR or Tempo Number	Vantive Case and/or Internal Reference Number	Description
V2.20	PEP0019735R	UNITY00046323	Enhancement to allow Modbus communication with radio modem and repeaters (from customer SAWS)
	PEP0026935R	UNITY00049170	BMXP342020-Self test adaptation and update status
	PEP0021128R	-	Evolution: a status to inform that an M340 application is protected with the SD card serial number mechanism or with a signature written on the SD card
	PEP0016573R	1108488	Bad behaviour of the embedded Modbus port when using Input_Byte or Input_char instruction
	PEP0020590R	1136809 UNITY00047136	When M340 CPU V2.0 is switched on, NetLink manager (ADDM with symbolic network name) doesn't return the correct result of NOE network name
	PEP0012532R PEP0015403R PEP0026690R	UNITY00048206	Evolution: to better substitute Compact applications, M340 supports additional system words %SW138 to %SW141: Offset Starting Address of Modbus requests
	PEP0028700R	1177344 1206691	An M340 CPU with an XBTGT connected on the USB port can stop after switching off the power supply several times
	PEP0031190R	1219629	An M340 CPU can stop when using Input_char and Print_char instructions in a specific manner

(*) BMXP342010 and BMXP342030 are no more manufactured.

M340 - BMX P34 1000 / P34 2000 / P34 2010/ P34 20102* / P34 2020 / P34 20302* / P34 2030 firmware history

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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 Number	OPR or Tempo Number	Vantive Case or Internal Reference Number	Description
V2.10	20040480	994155	Enhancement : possibility to disable Warm Start feature after power recycling (forcing a Cold Start)
	PEP0012863R	-	Delay before and after sending frames using RTS/CTS signals not well managed
	20043797	1081706	Management of Readbol request that was not allowed
	20044468	1093941	Animation issue in DFB section (programmed in FBD)
	20043923	1121176	No programming on PLC is possible because it was reserved by Empty Entity
	PEP0016838R	1110996, 1105393	CPU could fail after using Technical Support button in Unity Pro
	PEP0017008R	Unity00046144	Enhancement : activate / deactivate CANopen slaves status on M340 Master
	20044729	-	On a CPU P34 2020, a Modbus command for Web access to SMTP diagnostics halts the system
	20044849	1097282	BootP issue on CPU P34 2020
	20045201	1129515	When doing Read/Write_VAR repeatedly to IP address that is not on the network, the count of open connections goes to the max value and messages to a correct address are lost. The problem occurs on both the CPU and NOE modules

(*) BMXP342010 and BMXP342030 are no more manufactured.

M340 - BMX P34 1000 / P34 2000 / P34 2010/ P34 20102* / P34 2020 / P34 20302* / P34 2030 firmware history

Note: *Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends to all customers to ensure that their installation is up to date with the newest firmware versions, 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 Number	OPR Number	Vantive Case Number or Internal Reference Number	Description
V2.00	20041439	UNITY00039641	M340 CANopen master does not recover automatically from a bus-off state
	20041561	UNITY00039644	Using the M340, the %SW96 bits are set without writing to a %MW
	20041821	-	CANopen error during factory auto tests
	20042010	UNITY00039646	Execution of a SFC application causes a HALT of the processor or simulator
	20042549	-	%MW are restored from flash while the MAST task is running
	20042710	1031750	%MW are initialized on a warm start if "IF %S1 THEN SET %S0; END_IF;" is programmed in a Unity Pro section, whereas on the Premium the %MW values are kept.
	20041515	-	CANopen error if the EF Read_VAR buffer is too small
	20042517	UNITY00040320	PWM_INT behaviour is different under a simulator or a real CPU
	20042651	1026376 1030972 1048577	Modbus serial link issues with management of RTS/CTS modem signals
	20043557	-	Issue in the Unity Pro PLC Screen
	20043385	-	M340 CPU P34 2030 could not start after downloading a CANopen project

(*) BMXP342010 and BMXP342030 are no more manufactured.