Schneider Electric Security Notification

BadAlloc Vulnerabilities

09 November 2021 (10 January 2023)

Overview

Schneider Electric is aware of multiple memory allocation vulnerabilities dubbed 'BadAlloc', disclosed by Microsoft on April 29, 2021. The impact of a successful exploitation of the vulnerabilities may result in denial of service, or remote code execution, depending on the context.

January 2023 Update: There are remediations available for Easergy MiCOM P30 range (page 2) and Pro-face LT4000M Series (page 10).

Vulnerability Details

The complete list of affected real-time operating systems can be found here: https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04.

Affected Products, Remediations & Mitigations

Schneider Electric has determined that the following offers are impacted and has provided remediations, for those listed in the Available Remediations section, and recommended mitigations, for those in the Affected Products section.

Please subscribe to the Schneider Electric security notification service to be informed of critical updates to this notification, including information on affected products and remediation plans:

https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Remediations/Final Mitigations

Products & Affected Versions	CVEs	Remediation/Mitigation
Easergy C5x (C52/C53) *prior to V1.0.5*	CVE-2020-35198 CVE-2020-28895	Version 1.0.5 of Easergy C5 includes a fix for these vulnerabilities and is available through Schneider Electric regional DPACs.

Easergy MiCOM P30 range, models: C434, P132, P139, P433, P435, P437, P439, P532, P631, P632, P633, P634 *Versions 660 - 674*	CVE-2020-35198 CVE-2020-28895	Version 675 of the P30 firmware includes a fix for these vulnerabilities and is available on request from Schneider Electric's Customer Care Center.
Easergy P5 *V01.401.101 and prior*	CVE-2020-28895	Version 01.401.101 of Easergy P5 firmware includes a fix for this vulnerability and is available on request from Schneider Electric's Customer Care Center.
EPC2000 *V3.01 firmware version and prior*	CVE-2020-35198 CVE-2020-28895	Version 4.03 of the EPC2000 includes a fix for these vulnerabilities and is available for download here: https://www.eurotherm.com/?wpdmdl=137741
EPC3000 *V5.10 firmware version and prior*	CVE-2020-35198 CVE-2020-28895	Version 5.20 of the EPC3000 includes a fix for these vulnerabilities and is available for download here: https://www.eurotherm.com/?wpdmdl=89545 Device will reboot automatically after upgrade.
Easy Harmony ET6 (HMIET Series) *Vijeo Designer Basic V1.2 family and prior*	CVE-2020-28895 CVE-2020-35198	Version 1.2.1 of Vijeo Designer Basic includes a fix for these vulnerabilities. Please contact your Schneider Electric's Customer Care Center to obtain the installer. To complete the update, connect to Harmony HMI and download the firmware using Vijeo Designer Basic V1.2.1.
Easy Harmony GXU (HMIGXU Series) *Vijeo Designer Basic V1.2 family and prior*	CVE-2020-28895 CVE-2020-35198	Version 1.2.1 of Vijeo Designer Basic includes a fix for these vulnerabilities. Please contact your Schneider Electric's Customer Care Center to obtain the installer. To complete the update, connect to Harmony HMI and download the firmware using Vijeo Designer Basic V1.2.1.

Eurotherm E+PLC100 *All Versions*	CVE-2020-35198 CVE-2020-28895	The E+PLC100 product has reached its end of life and is no longer supported. Customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to the device. • Configure the Access Control List following the recommendations of the device user manual. • Setup a VPN between the E+PLC100 device and any remote visualization workstations running the E+PLC tools. • Activate and apply user management and password features. Limit the access to both development and control system by physical means, operating system features, etc.
Eurotherm E+PLC400 *V1.3.0.1 and prior*	CVE-2020-35198 CVE-2020-28895	Version 1.4.0.0 of the E+PLC400 firmware is available and includes a fix for these vulnerabilities. Please contact the Eurotherm Support team to obtain the firmware update. Please be sure to include the following when contacting the support team: • End Username, Company, and Email Address • Serial numbers of the devices to be upgraded • Current E+PLC400 firmware version
Eurotherm Eycon 10/20 Visual Supervisor *V7.2 and prior*	CVE-2020-35198 CVE-2020-28895	Version 7.3 of the Eycon firmware is available and includes a fix for these vulnerabilities. Access to the patch can be obtained through the following link: https://partners.eurotherm.com/member-login
Eurotherm T2550 PAC *V8.1 and prior*	CVE-2020-35198 CVE-2020-28895	Version 8.2 of the T2550 firmware is available and includes a fix for these vulnerabilities. Access to the patch can be obtained through the following link: https://partners.eurotherm.com/member-login

Eurotherm T2750 PAC *V6.2 and prior*	CVE-2020-35198 CVE-2020-28895	Version 6.3 of the T2750 firmware is available and includes a fix for these vulnerabilities. Access to the patch can be obtained through the following link: https://partners.eurotherm.com/member-login
Harmony/ Magelis HMIGTU Series **HMIGTUX Series** **HMIGK Series** *Vijeo Designer V6.2 SP11 Hotfix 3 and prior*	CVE-2020-35198 CVE-2020-28895	Version 6.2 SP11 Multi HotFix 4 of Vijeo Designer includes a fix for these vulnerabilities and can be updated through the Schneider Electric Software Update (SESU) application. On the engineering workstation, update to V6.2 SP11 Multi HotFix 4 (or above) of Vijeo Designer. In order to complete the update, connect to Harmony HMI and download the project file using Vijeo Designer V6.2 SP11 Multi HotFix 4.
HMISCU *Vijeo Designer V6.2 SP11 and prior*	CVE-2020-28895 CVE-2020-35198	Version 6.2 SP12 of Vijeo Designer includes a fix for these vulnerabilities and can be updated through the Schneider Electric Software Update (SESU) application. On the engineering workstation, update to V6.2 SP12 (or above) of Vijeo Designer. To complete the update, connect to Harmony HMI and download the project file using Vijeo Designer V6.2 SP12.

JACE-8000 *All TAC I/A Series Niagara Framework® platforms prior to Niagara 4.8 are impacted*	CVE-2021-22156	Updates have been released to address the identified vulnerability Customers are urged to upgrade to Niagara 4.10u1. These updates are available on the Schneider Electric Exchange or by contacting your sales support channel or by contacting the Schneider Electric support team at productsupport.NAM-BMS@schneider-electric.com. It is important that all TAC I/A Series Niagara customers for all supported platforms update their systems with these releases to mitigate risk. If you have any questions, please contact your Schneider Electric support team at productsupport.NAM-BMS@schneider-electric.com. As always, we highly recommend that TAC I/A Series Niagara customers running on an unsupported platform (such as Niagara G3/AX) take action to update their systems to a supported platform, ideally the 4.10u1 release of Niagara Framework. In addition to updating your system, Schneider Electric recommends that customers with affected products take the following steps to protect themselves: • Review and validate the list of users who are authorized and who can authenticate to Niagara. • Allow only trained and trusted persons to have physical access to the system, including devices that have connection to the system though the Ethernet port. • Consider using a VPN or other means to ensure secure remote connections into the network where the system is located, If remote connections are enabled. • Sign all modules and program objects provided by third-party teams. Review the Niagara Hardening Guide for techniques on securing your installation.
MiCOM C264 *B5.x up to B5.118* *D1.x up to D1.92* *D4.x up to D4.38* *D5.x up to D5.25l* *D6.x up to D6.18*	CVE-2020-35198 CVE-2020-28895	Versions *B5.118, D1.92, D4.38, D5.25l and D6.18* of MiCOM C264 include a fix for these vulnerabilities and are available through Schneider Electric regional DPACs.

Modicon M241/M251 Logic Controllers *Firmware V 5.1.9.34 and prior*	CVE-2020-28895 CVE-2020-35198	Version 5.1.9.34 of Modicon M241/M251 Logic Controllers includes a fix for these vulnerabilities. On the engineering workstation, update to latest version of EcoStruxure Machine Expert: https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-somachine/?parent-subcategory-id=5140&filter=business-1-industrial-automation-and-control To complete the update on Modicon M241/M251 Logic Controllers, update to firmware version V5.1.9.34 or higher available within EcoStruxure Machine Expert. A reboot is needed.
Modicon M262 Logic Controllers *Firmware prior to V5.1.6.1*	CVE-2020-28895 CVE-2020-35198	Version 5.1.6.1 of Modicon M262 Logic Controllers includes a fix for these vulnerabilities. On the engineering workstation, update to latest version of EcoStruxure Machine Expert: https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-somachine/?parent-subcategory-id=5140&filter=business-1-industrial-automation-and-control To complete the update on Modicon M262 Logic Controllers, update to firmware version V5.1.6.1 or higher available within EcoStruxure Machine Expert. A reboot is needed.
Modicon M258/ LMC058 Logic Controllers *Firmware prior than V5.0.4.18*	CVE-2020-28895 CVE-2020-35198	Firmware Version 5.0.4.18 of Modicon M258/LMC058 logic controllers includes a fix for these vulnerabilities and can be updated through Schneider Electric Software Update (SESU) application.
Modicon M340 Module BMXNOC0401 *prior to V2.11*	CVE-2020-35198 CVE-2020-28895	Version 2.11 of BMXNOC0401 includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/BMXNOC0401/
Modicon M340 Module BMXNOR0200H RTU *prior to V1.7 IR24*	CVE-2020-35198 CVE-2020-28895	Version 1.7 IR24 of BMXNOR0200H includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/BMXNOR0200H/

Modicon M340 CPU (BMXP34*) *V3.40 and prior*	CVE-2020-35198 CVE-2020-28895	Version 3.50 of Modicon M340 includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/download/document/BMXP34xxxxx_SV_03.50/
Modicon MC80 Controller (BMKC8*) *prior to V1.8*	CVE-2020-35198 CVE-2020-28895	Version 1.8 of MC80 Controller (BMKC80) includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/62396-modicon-mc80/#software-and-firmware
Modicon Momentum ENT (170ENT11*) *All versions*	CVE-2020-35198 CVE-2020-28895	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to the device. • Configure the Access Control List following the recommendations in the device user manual. • Setup a VPN between the Modicon PLC device and the remote engineering workstations. • Activate and apply user management and password features. • Limit the access to both development and control system by physical means, operating system features, etc.
Modicon Quantum CPU and Communication Modules *All Versions*	CVE-2020-28895 CVE-2020-35198	Quantum and Premium offers have reached their end of life and are no longer supported. Customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to the device. • Setup a VPN between the Modicon PLC device and the remote engineering workstations. • Activate and apply user management and password features. • Limit the access to both development and control system by physical means, operating system features, etc. Customers should also consider upgrading to the latest product offering Modicon M580 ePAC.

Modicon Premium CPU and Communication Modules *All Versions*	CVE-2020-28895 CVE-2020-35198	Quantum and Premium offers have reached their end of life and are no longer supported. Customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to the device. • Setup a VPN between the Modicon PLC device and the remote engineering workstations. • Activate and apply user management and password features. • Limit the access to both development and control system by physical means, operating system features, etc. Customers should also consider upgrading to the latest product offering Modicon M580 ePAC.
nanodac *V9.01 firmware version and prior*	CVE-2020-28895 CVE-2020-35198	Version 10.02 of nanodac includes a fix for this vulnerability and is available for download here: https://www.eurotherm.com/?wpdmdl=28419 Device will reboot automatically after upgrade.
PacDrive Eco/Pro/Pro2 Logic Controllers *Firmware versions prior to V1.66.5.1*	CVE-2020-28895 CVE-2020-35198	Firmware Version 1.66.5.1 of PacDrive Eco/Pro/Pro2 Logic Controllers includes a fix for these vulnerabilities and can be updated through the Schneider Electric Software Update (SESU) application.

PacDrive M *All Versions*	CVE-2020-28895 CVE-2020-35198	PacDrive M Logic Controller has reached its end of life and is no longer supported. Customers should immediately apply the following mitigations to reduce the risk of exploit: • Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside, • Use firewalls to protect and separate the control system network from other networks, • Use VPN (Virtual Private Networks) tunnels if remote access is required, • Activate and apply user management and password features, • Limit the access to both development and control system by physical means, operating system features, etc. Customers should also consider upgrading to the latest product offering PacDrive Eco/Pro/Pro2 to resolve this issue.
PowerLogic ION7400 *Firmware V3.0 and prior*	CVE-2020-35198 CVE-2020-28895	Version 3.1 of PowerLogic ION7400 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/ION7400_meter_FW_v003.001.000/ If the update cannot be applied immediately, please follow the guidelines in Schneider Electric Recommended Cybersecurity Best Practices document to help mitigate the risk.
PowerLogic PM8000 *Firmware V3.0 and prior*	CVE-2020-35198 CVE-2020-28895	Version 3.1 of PowerLogic PM8000 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/PM8000_meter_FW_v003.001.000/ If the update cannot be applied immediately, please follow the guidelines in Schneider Electric Recommended Cybersecurity Best Practices document to help mitigate the risk.

PowerLogic ION9000 *Firmware V3.0 and prior*	CVE-2020-35198 CVE-2020-28895	Version 3.1 of PowerLogic ION9000 includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/ION9000_meter_FW_v003.001.000/ If the update cannot be applied immediately, please follow the guidelines in Schneider Electric Recommended Cybersecurity Best Practices document to help mitigate the risk.
Pro-face SP-5B00, SP-5B10, SP-5B90, ST6000 Series (GP-ProEX model), ET6000 Series *GP-Pro EX V4.09.300 and prior*	CVE-2020-35198 CVE-2020-28895	Version 4.09.350 of Pro-face GP-Pro EX includes a fix for these vulnerabilities and is available for download here: https://www.proface.com/en/download/trial/gpproex/v40 or update online via GP-Pro EX (refer to Help menu and select “Confirm Update of GP-Pro EX”). To complete the update, connect to Pro-face HMI and download the project file using GP-Pro EX V4.09.350 or later.
Pro-face LT4000M Series GP-Pro EX *V4.09.400 and prior*	CVE-2020-35198 CVE-2020-28895	Version 4.09.450 of Pro-face GP-Pro EX includes a fix for these vulnerabilities and is available for download here: https://www.proface.com/en/download/trial/gpproex/v40 or update online via GP-Pro EX (refer to Help menu and select “Confirm Update of GP-Pro EX”). To complete the update, connect to Pro-face HMI and download the project file using GP-Pro EX V4.09.450 or later.
Pro-face GP4000 Series, GP4000H Series GP-Pro EX *V4.09.350 and prior*	CVE-2020-35198 CVE-2020-28895	Version 4.09.400 of Pro-face GP-Pro EX includes a fix for these vulnerabilities and is available for download here: https://www.proface.com/en/download/trial/gpproex/v40 or update online via GP-Pro EX (refer to Help menu and select “Confirm Update of GP-Pro EX”). To complete the update, connect to Pro-face HMI and download the project file using GP-Pro EX V4.09.400 or later.

Profibus Remote Master TCSEGPA23F14F, BMECXM0100 *All versions*	CVE-2020-35198 CVE-2020-28895	Customers should immediately apply the mitigations found in the Cybersecurity Reference Manual linked below to reduce the risk of exploit: https://www.se.com/ww/en/download/document/EIO0000001999/
SCD6000 Industrial RTU *Version SCD6000 SY1101211_M and prior*	CVE-2020-35198 CVE-2020-28895	Version *SY-1101207, Version N* of *SCD6000 firmware* includes a fix for this vulnerability. Contact your local Customer Support to receive this firmware version. Reboot is required after installation.
SAGE RTU CPU C3414 *All versions prior to C3414-500-S02K5_P5*	CVE-2020-35198 CVE-2020-28895	Version C3414-500-S02K5_P5 of SAGE RTU CPU 3414 includes a fix for this vulnerability and is available for download here: https://www.sage-rtu.com/downloads.html Reboot of SAGE RTU is required after firmware upgrade. This fix applies a Wind River VxWorks (real-time operating system) patch to bring code libraries current to 6.9.4.12 RCPL3 revision. This corrects issues with overflow causing malloc/calloc to return valid pointer when it should return fail indication NULL pointer.
Versadac *Versions prior to Version 2.41 firmware*	CVE-2020-35198 CVE-2020-28895	Version 2.43 of the Versadac scalable data recorder is available and includes a fix for these vulnerabilities. Access to the patch can be obtained through the following link: https://partners.eurotherm.com/member-login

Affected Products

Schneider Electric is currently establishing a remediation plan for the following products. This document will be updated when product specific information is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit.

Please subscribe to the Schneider Electric security notification service to be informed of critical updates to this notification, including information on affected products and remediation plans:
https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's Customer Care Center.

Recommended Mitigations

Products	CVEs	Recommended Mitigation
BMECRA31210, BMXCRA31200, BMXCRA31210, 140CRA31200, 140CRA31908 *All versions*	CVE-2020-35198 CVE-2020-28895	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to the device. • Configure the Access Control List following the recommendations of the device user manual. • Setup a VPN between the Modicon. Communication modules and the remote engineering workstations. • Activate and apply user management and password features. • Limit the access to both development and control system by physical means, operating system features, etc.
BMXNOE0100, BMXNOE0110, BMXNGD0100, *All versions*		
BMENOC0301, BMENOC0311, BMENOC0321, BMENOS0300, *All versions*		
BMENOP0300 *All versions*		
BMXNOM0200 *All versions*	CVE-2020-35198, CVE-2020-28895	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Configure the Access Control List in the Modicon controller associated to this module following the recommendations of the device user manual. • Limit the access to both development and control system by physical means, operating system features, etc.
Easergy MiCOM P30 range, model *Px36/8* *Versions 660 - 674*	CVE-2020-35198, CVE-2020-28895	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Use relays only in a protected environment to minimize network exposure and ensure that they are not accessible from outside. • Disable unused network protocol interfaces. • Use firewalls to protect and separate the control system network from other networks. • Activate and apply user management and password features.

Easergy MiCOM P40 *All versions*	CVE-2020-28895	• Limit the access to the system by physical means.
EPack *All versions*	CVE-2020-35198 CVE-2020-28895	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to the device. • Configure the Access Control List following the recommendations of the device user manual. • Setup a VPN between the EPack device and any remote visualization workstations running iTools. • Activate and apply user management and password features. Limit the access to both development and control system by physical means, operating system features, etc.
HMISTO Series **HMISTU/S5T Series** *All versions*	CVE-2020-35198 CVE-2020-28895	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network. • Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks. • Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet. When remote access is required, use secure methods, such as the Vijeo Connect.

Modicon M580 CPU (BMEP* and BMEH*)
All versions
	CVE-2020-35198
	CVE-2020-28895
		Modicon M580 SV4.02 firmware has been retracted for quality issues and is no longer available for download. For specific questions or support, Customers are requested to contact Schneider Electric's Customer Care Center
		
		Customers should immediately apply the following mitigations to reduce the risk of exploit:
		• Configure the Access Control List following the recommendations of the user manuals:
		  ○ "Modicon M580, Hardware, Reference Manual": https://www.se.com/ww/en/download/document/EIO0000001578/
		• Setup a secure communication according to the following guideline "Modicon Controllers Platform Cyber Security Reference Manual," in chapter "Setup secured communications": https://www.se.com/ww/en/download/document/EIO0000001999/
		• Use a BMENUA0100 module and follow the instructions to configure IPSEC feature as described in the chapter "Configuring the BMENUA0100 Cybersecurity Settings": https://www.se.com/ww/en/download/document/PHA83350
		• Ensure the CPU is running with the memory protection activated by configuring the input bit to a physical input, for more details refer to the following guideline "Modicon Controllers Platform Cyber Security Reference Manual", "CPU Memory Protection section": https://www.schneider-electric.com/en/download/document/EIO0000001999/
		  ○ NOTE: The CPU memory protection cannot be configured with Hot Standby CPUs. In such cases, use IPsec encrypted communication.

M580 CPU Safety BMEP58*S and BMEH58*S *All versions*	CVE-2020-35198 CVE-2020-28895	Schneider Electric is establishing a remediation plan for all future versions of Modicon M580 CPU Safety BMEP58*S and BMEH58*S that will include a fix for these vulnerabilities. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Configure the Access Control List following the recommendations of the user manuals: ○ "Modicon M580, Hardware, Reference Manual": https://www.se.com/ww/en/download/document/EIO0000001578/ • Setup a secure communication according to the following guideline "Modicon Controllers Platform Cyber Security Reference Manual," in chapter "Setup secured communications": https://www.se.com/ww/en/download/document/EIO0000001999/ • Use a BMENUA0100 module and follow the instructions to configure IPSEC feature as described in the chapter "Configuring the BMENUA0100 Cybersecurity Settings": https://www.se.com/ww/en/download/document/PHA83350 To further reduce the attack surface on Modicon M580 CPU Safety: • Ensure the CPU is running in Safety mode and maintenance input is configured to maintain this Safety mode during operation – refer to the document Modicon M580 - Safety System Planning Guide - in the chapter "Operating Mode Transitions": https://www.se.com/ww/en/download/document/QGH60283/

Modicon LMC078 *All versions*	CVE-2020-28895 CVE-2020-35198	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside, • Use firewalls to protect and separate the control system network from other networks, • Use VPN (Virtual Private Networks) tunnels if remote access is required, • Activate and apply user management and password features, • Limit the access to both development and control system by physical means, operating system features, etc. Customers should also consider upgrading to the latest product offering Modicon M262 to resolve this issue.
Pro-face GP4100 Series, GP4000E Series, GP4000M Series *All versions*	CVE-2020-35198, CVE-2020-28895	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network. • Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks. • Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet. • When remote access is required, use secure methods, such as the Pro-face Connect. Customers should also consider upgrading to the latest product offering to resolve this issue. Please contact your sales support about alternative products

6100A, **6180A,** **6100XIO,** **6180XIO,** **AeroDAQ** *All versions*	CVE-2020-35198 CVE-2020-28895	Customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to the device. • Configure the Access Control List following the recommendations of the device user manual. • Setup a VPN between the 6000-series device and any remote visualization workstations running Bridge. • Activate and apply user management and password features. Limit the access to both development and control system by physical means, operating system features, etc.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the “Program” mode.
- Never connect programming software to any network other than the network intended for that device.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact

your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.

www.se.com

Schneider Electric Security Notification

Revision Control

Version 1.0 *09 November 2021*	Original Release
Version 1.1 *17 November 2021*	Fixed version number of PacDrive Eco/Pro/Pro2 Logic Controllers corrected to V1.66.5.1.
Version 2.0 *14 December 2021*	Remediations added for SCD6000 Industrial RTU, PowerLogic ION7400, PowerLogic ION8000, PowerLogic ION9000. Upon further investigation Tricon Communication Modules have been removed from list of affected products and are not impacted by the Badalloc Vulnerabilities.
Version 3.0 *15 December 2021*	Remediations added for PowerLogic ION9000.
Version 4.0 *11 January 2022*	Remediations added for Easergy P5, EPC3000, Harmony/ Magelis HMIGTU Series, HMIGTUX Series, HMIGK Series, nanodac, Pro-face SP-5B00, SP-5B10,SP-5B90,ST6000 Series (GP-ProEX model), ET6000 Series in the Available Remediations section (page 1, 2, 4, and 6). Updated versions affected to all versions for Pro-face GP4000 Series, LT4000M Series, GP4000H Series in the Affected Versions section.
Version 4.1 *13 January 2022*	Moved back to affected products section: Harmony/ Magelis HMIGTU Series, HMIGTUX Series, HMIGK Series.
Version 5.0 *08 February 2022*	Available remediations for Easy Harmony ET6 (HMIET Series), Easy Harmony GXU (HMIGXU Series), Harmony/ Magelis (HMIGTU Series, HMIGTUX Series, HMIGK Series), Modicon M262 Logic Controllers, and Modicon M241/M251 Logic Controllers. Added Easergy MiCOM P30 and Easergy MiCOM P40 to the list of affected products.
Version 6.0 *12 April 2022*	Added remediations for Eurotherm E+PLC400, Eurotherm T2750 PAC and Modicon M340 CPU. Additionally, Eurotherm T2550 PAC and Eurotherm Eycon 10/20 Visual Supervisor have been added as affected products to this security notification in the remediation section.
Version 7.0 *10 May 2022*	Added a remediation for HMISCU, added the following affected models to the Easergy MiCOM P30 range: C434, P132, P139, P433, P435, P437, P532, P631, P632, P633, P634, Px36/8.
Version 8.0 *14 June 2022*	Added a remediation for EPC2000, V4.03 includes a fix.
Version 9.0 *15 June 2022*	Remediation added for Versadac. The previously added remediation for EPC2000 has been removed as V4.03 is not

	yet available, this document will be updated when it is released.
Version 10.0 *09 August 2022*	Remediations available for Modicon M580 CPU (BMEP* and BMEH*) and Pro-face GP4000 Series, GP4000H Series GP-Pro EX.
Version 11.0 *13 September 2022*	Final Remediations available for Modicon M340 Modules BMXNOC0401 and BMXNOR0200H RTU, and Modicon MC80 Controller (BMKC8*). There is a mitigation available for Profibus Remote Master (TCSEGPA23F14F) and CANopen X80 Communication Module (BMECXM0100).
Version 12.0 *11 October 2022*	Easergy MiCOM P30 range P632 and P633 were added as affected models along with a remediation. Final mitigations were added for Modicon Momentum ENT. Adding a clarification to the list of affected products by splitting Modicon M580 and Modicon M580 Safety CPU ranges; the latest fix Modicon M580 V4.02 does not apply to the Safety range of M580.
Version 13.0 *08 November 2022*	A remediation is now available for EPC2000.
Version 14.0 *13 December 2022*	The Modicon M580 SV4.02 firmware has been retracted for quality issues and is no longer available for download. Additional mitigations have been introduced for Modicon M580 CPU and M580 CPU Safety, and we urge customers to deploy these mitigations to further reduce the risk of potential exploitation of identified vulnerabilities.
Version 15.0 *10 January 2023*	There are remediations available for Easergy MiCOM P30 range (page 2) and Pro-face LT4000M Series (page 10).

Product Security Office

Digitally signed by Product Security Office
Date: 2023.01.11 06:51:41 -05'00'