

# Schneider Electric Security Notification

## Treck TCP/IP Vulnerabilities (Ripple20) (V2.8)

23 June 2020 (18 December 2020)

### Overview

Schneider Electric is aware of multiple vulnerabilities affecting Treck Inc.'s embedded TCP/IP stack, collectively known as Ripple20, which Treck disclosed publicly on June 16. The vulnerabilities range in severity and therefore have varying levels of risk.

Schneider Electric continues to assess how the newly disclosed vulnerabilities affect its offers. The company will continue to update this notification as additional offer-specific information becomes available.

Customers should immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves from possible exploitation of these vulnerabilities. Where appropriate, this includes locating their industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission-critical systems and devices from being accessed from outside networks; and following the remediation and general security recommendations below.

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

### Affected Products & Remediations

**Schneider Electric has determined that the following offers are impacted. The company will update this table as it continues to assess the impact these vulnerabilities have on its offers.**

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>

## Schneider Electric Security Notification

### Available Remediations

Industrial Automation Products	Affected Versions	Remediation/Mitigation
ATV340E Altivar Machine Drives	All Versions prior to V3.2IE25	A fix is now available in product releases V3.2IE25 and above. For product release prior to V3.2IE25, apply the mitigations detailed in the Recommended Mitigations section and contact your <a href="#">local technical support</a> for more information.
ATV630/650/660/680/6A0/6B0 Altivar Process Drives	All Versions prior to V3.3IE33	A fix is now available in product releases V3.3IE33 and above. For product release prior to V3.3IE33, apply the mitigations detailed in the Recommended Mitigations section and contact your <a href="#">local technical support</a> for more information.
ATV930/950/960/980/9A0/9B0 Altivar Process Drives	All Versions prior to V3.3IE26	A fix is now available in product releases V3.3IE26 and above. For product release prior V3.3IE26, apply the mitigations detailed in the Recommended Mitigations section and contact your <a href="#">local technical support</a> for more information.
SCADAPack 32 RTU	All versions prior to V2.25	Telepace Studio must be used to update the SCADAPack 32 RTU firmware to version 2.25 or newer.  Download and install Telepace Studio 5.4.2 or newer from <a href="https://shop.exchange.se.com/en-US/apps/55670">https://shop.exchange.se.com/en-US/apps/55670</a>
TM3BC bus coupler module – EIP	All versions prior to V2.1.50.2	<a href="#">CVE-2020-11896</a> and <a href="#">CVE-2020-11898</a> have been fixed in the TM3BCEIP Firmware Update V2.1.50.2 available for download below: <a href="https://www.se.com/ww/en/download/document/TM3BCEIP_Firmware_Update/">https://www.se.com/ww/en/download/document/TM3BCEIP_Firmware_Update/</a>  This table will be updated when remediations are available for the remaining CVEs.

## Schneider Electric Security Notification

<p>TM3BC bus coupler module - SL</p>	<p>All versions prior to V2.0.50.2</p>	<p><a href="#">CVE-2020-11896</a> and <a href="#">CVE-2020-11898</a> have been fixed in the TM3BCSL Firmware Update V2.0.50.2 available for download below:  <a href="https://www.se.com/ww/en/download/document/TM3BCSL_Firmware_Update/">https://www.se.com/ww/en/download/document/TM3BCSL_Firmware_Update/</a></p> <p>This table will be updated when remediations are available for the remaining CVEs.</p>
<p>TM3BC bus coupler module - CANOpen</p>	<p>All versions prior to V2.0.50.2</p>	<p><a href="#">CVE-2020-11896</a> and <a href="#">CVE-2020-11898</a> have been fixed in the TM3BCCO Firmware Update V2.0.50.2 available for download below:  <a href="https://www.se.com/ww/en/download/document/TM3BCCO_Firmware_Update/">https://www.se.com/ww/en/download/document/TM3BCCO_Firmware_Update/</a></p> <p>This table will be updated when remediations are available for the remaining CVEs.</p>
<p>VW3A3310 Altivar 61/71 Modbus TCP option</p>	<p>All Versions (V2.11E09 and prior)</p>	<p>This is an End Of Commercialization offer that is replaced by the <a href="#">ALTIVAR 900</a> &amp; <a href="#">ALTIVAR 600</a> ranges.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the <a href="#">Recommended Mitigations</a> section.</p>
<p>VW3A3310D Altivar 61/71 Ethernet daisy chain option</p>	<p>All Versions (V3.01E11 and prior)</p>	<p>This is an End Of Commercialization offer that is replaced by the <a href="#">ALTIVAR 900</a> &amp; <a href="#">ALTIVAR 600</a> ranges.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the <a href="#">Recommended Mitigations</a> section.</p>
<p>VW3A3316 Altivar 61/71 Ethernet IP option</p>	<p>All Versions (V1.21E14 and prior)</p>	<p>This is an End Of Commercialization offer that is replaced by the <a href="#">ALTIVAR 900</a> &amp; <a href="#">ALTIVAR 600</a> ranges.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the <a href="#">Recommended Mitigations</a> section.</p>

## Schneider Electric Security Notification

<p>VW3A3320 Altivar 61/71 Ethernet IP RSTP option</p>	<p>All Versions (V1.11E19 and prior)</p>	<p>This is an End Of Commercialization offer that is replaced by the <a href="#">ALTIVAR 900</a> &amp; <a href="#">ALTIVAR 600</a> ranges.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the <a href="#">Recommended Mitigations</a> section.</p>
<p>XUPH001 OsSense communication module</p>	<p>All versions</p>	<p>This offer is not affected by CVE-2020-11897, CVE-2020-11899, CVE-2020-11900, CVE-2020-11902, CVE-2020-11903, CVE-2020-11905, CVE-2020-11908, CVE-2020-11913.</p> <p>For other CVEs, the CVSS score is evaluated as Medium in the product context.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the <a href="#">Recommended Mitigations</a> section.</p>
<p>XGCS850C201 OsiSense RFID compact smart antenna</p>	<p>All versions</p>	<p>This offer is not affected by CVE-2020-11897, CVE-2020-11899, CVE-2020-11900, CVE-2020-11902, CVE-2020-11903, CVE-2020-11905, CVE-2020-11908, CVE-2020-11913.</p> <p>For other CVEs, the CVSS score is evaluated as Medium in the product context.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the <a href="#">Recommended Mitigations</a> section.</p>
<p>VW3A3720, VW3A3721 Altivar Process Communication Modules</p>	<p>All Versions prior to V1.15IE25</p>	<p>A fix is available in product releases V1.15IE25 and above.</p> <p>For product release prior V1.15IE25, apply the mitigations detailed in the Recommended Mitigations section and contact your <a href="#">local technical support</a> for more information.</p>

## Schneider Electric Security Notification

Energy Management Products	Affected Versions	Remediation/Mitigation
ACE850 Sepam communication interface	All versions	<p>The ACE850 ethernet module for SEPAM protection relays is a product designed to be operated on a secure network.</p> <p>To minimize the risk from both Ripple 20 and the network-accessible functions of the relay we recommend that concerned customers:</p> <ul style="list-style-type: none"> <li>- Enable the IP-based filtering capability in the ACE850</li> <li>- Place strong, active controls on the network hosting the ACE850</li> <li>- Consider moving to a newer relay such as the Easergy series if product-level access protections are required</li> </ul> <p>To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.</p>
Acti9 Smartlink IP	All versions	<p>This is an End of Commercialization offer. If possible, this product should be replaced by Smartlink SIB (commercial reference : A9XMZA08) for which a patch is available in FW version 2.18 or greater.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.</p>
Acti9 PowerTag Link / HD	Versions prior to 001.008.007	<p>Customers should update firmware using EcoStruxure Power Commission (EPC) installer V7.0 available here:  <a href="https://www.se.com/ww/en/product-range-download/64482-acti9-powertag-link/?selected-nodeid=12492093362#/software-firmware-tab">https://www.se.com/ww/en/product-range-download/64482-acti9-powertag-link/?selected-nodeid=12492093362#/software-firmware-tab</a></p>
Acti9 Smartlink SI D	Versions prior to 002.004.002	<p>Customers should update firmware using EcoStruxure Power Commission (EPC) installer V7.0 available here:  <a href="https://www.se.com/ww/en/product-range-download/64482-acti9-powertag-link/?selected-nodeid=12492093362#/software-firmware-tab">https://www.se.com/ww/en/product-range-download/64482-acti9-powertag-link/?selected-nodeid=12492093362#/software-firmware-tab</a></p>
Acti9 Smartlink SI B		

## Schneider Electric Security Notification

EGX150/Link150 Ethernet Gateway	V5.1.15 and prior	A fix is available in V5.1.18: <a href="https://www.se.com/ww/en/product-range-download/63423-link150/?selected-node-id=12366756685">https://www.se.com/ww/en/product-range-download/63423-link150/?selected-node-id=12366756685</a> - /software-firmware-tab
eIFE Ethernet Interface for MasterPact MTZ drawout circuit breakers	Firmware versions earlier than V4.001.000	The firmware is available through EcoStruxure Power Commission (EPC) software V2.18. The updated version of EPC is available here: <a href="https://www.se.com/ww/en/download/document/Ecoreach_Installer/">https://www.se.com/ww/en/download/document/Ecoreach_Installer/</a>
EcoStruxure Building SmartX IP MP Controllers	All versions	All issues remediated in the 3.02.01 release, and higher. Update files can be found on the Schneider Electric Exchange <a href="https://ecoxpert.se.com/">https://ecoxpert.se.com/</a> -- <ol style="list-style-type: none"> <li>1. Search for 'relebov3.2.1'</li> <li>2. Set the Filter criteria to RN or Firmware, as required.</li> </ol>
EcoStruxure Building SmartX IP RP Controllers	All versions	All issues remediated in the 3.02.01 release, and higher. Update files can be found on the Schneider Electric Exchange <a href="https://ecoxpert.se.com/">https://ecoxpert.se.com/</a> <ol style="list-style-type: none"> <li>1. Search for 'relebov3.2.1'</li> <li>2. Set the Filter criteria to RN or Firmware, as required.</li> </ol>
IFE Ethernet Interface for ComPact, PowerPact, and MasterPact circuit breakers	Firmware versions earlier than V4.001.000	The firmware is available through EcoStruxure Power Commission (EPC) software V2.18. The updated version of EPC is available here: <a href="https://www.se.com/ww/en/download/document/Ecoreach_Installer/">https://www.se.com/ww/en/download/document/Ecoreach_Installer/</a>
IFE Gateway	Firmware versions earlier than V3.011.003	The firmware is available through EcoStruxure Power Commission (EPC) software V2.18. The updated version of EPC is available here: <a href="https://www.se.com/ww/en/download/document/Ecoreach_Installer/">https://www.se.com/ww/en/download/document/Ecoreach_Installer/</a>

## Schneider Electric Security Notification

PowerLogic EGX100 Ethernet Gateway	Versions 3.0 and newer	This is an End of Commercialization offer. If possible, this product should be replaced by Link 150 (commercial reference: EGX150) for which a patch is available in FW version 5.1.18 or greater. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
PowerLogic EGX300 Ethernet Gateway	All versions	This is an End of Commercialization offer. If possible, this product should be replaced by Com'X510 (commercial reference: EBX510) which is not impacted by this vulnerability. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
<p><b>APC Network Management Card 1 (NMC1) - AP9617, AP9618, AP9619</b> Devices with an embedded Network Management Card 1 include (but are not limited to): Metered/Switched Rack PDUs (AP78XX, AP79XX), Rack Automatic Transfer Switches (AP77XX), Environmental Monitoring Units (AP9320, AP9340, NetBotz 200).</p> <p><b>APC Network Management Card 2 (NMC2) - AP9630/30CH/30J, AP9631/31CH/31J, AP9635/35CH, AP9537SUM</b> Devices with an embedded Network Management Card 2 include (but are not limited to): 2G Metered/Switched Rack PDUs (AP84XX, AP86XX, AP88XX, AP89XX), Rack Automatic Transfer Switches (AP44XX), Certain Audio/Video Network Management Enabled products, Smart-UPS Online (SRT).</p> <p><b>APC Network Management Card 3 (NMC3) - AP9640, AP9641</b></p>		<p>Refer to <a href="#">Security Notification SEVD-2020-174-01</a> document for remediation and mitigations on all APC Network Management Card models.</p>

### Affected Products

Industrial Automation Products	Affected Version
ATV6000 Medium Voltage Altivar Process Drives	All Versions (V1.1IE02 and earlier)

## Schneider Electric Security Notification

TM3BC bus coupler module - EIP	All Versions
TM3BC bus coupler module - SL	All Versions
TM3BC bus coupler module - CANOpen	All Versions
ZBRCETH Modbus TCP communication module for ZBRN1 Harmony Hub	All Versions (V02.03 and earlier)
<b>Energy Management Products</b>	<b>Affected Version</b>
Acti9 PowerTag Link C	All versions
Acti9 Smartlink EL B	All versions
Acti9 Smartlink EL D	All versions
PowerLogic PM5000 series power meters	All versions
TeSys T LTMR08EBD Motor Controller	All versions
Wiser Energy IP module by Schneider Electric (EER31800)	All versions
Wiser Energy IP module by Clipsal (EER72600)	All versions
Gateway Connector by Elko (EKO01827)	All versions
Andover Continuum controller models: <ul style="list-style-type: none"> <li>- NetController 1 (NC1) = Model CX9900</li> <li>- NetController 2 (NC2) = Model CX9680</li> <li>- ACX2 = Model ACX5720 and ACX5740</li> <li>- CX9200 series</li> <li>- CX9400 series</li> <li>- CX9924</li> <li>- CX9702</li> <li>- BCX4040 series</li> </ul> BCX9640 series	All versions



# Schneider Electric Security Notification

## Recommended Mitigations

Since the vulnerabilities are present in the TCP/IP stack, an active network connection is required to exploit them. Therefore, Schneider Electric customers can act now to mitigate the risk of attack by limiting access to their devices.

For devices on a local network:

- Network Partitioning: Locate devices behind firewalls capable of deep packet inspection with rulesets limiting access with only approved protocols and functions and to only those devices and endpoints requiring access.
- Anomalous IP traffic: Block and detect anomalous IP traffic and malformed packets. Refer to the Solution section of the CERT-Coordination Center [Vulnerability Note VU#257161](#) for details.
- Disable DHCP on the NMC and configure it to use a static IP address.
- To avoid the use of DNS, set DNS servers to 0.0.0.0 and utilize static IP addresses for all servers the NMC will connect.
- If DNS must be used, then normalize DNS through a secure recursive server or application layer firewall
- Enable only secure remote access methods. Disable any insecure protocols.

For devices that must communicate via the Internet:

- Minimize network exposure for embedded and critical devices, keeping exposure to the minimum necessary, and ensuring that devices are not accessible from the Internet unless absolutely essential.

If network access is not required:

- Remove the Ethernet cable from the affected device.

Additional mitigations:

- Access Controls: Install physical and logical controls so no unauthorized personnel or device can access your systems, components, peripheral equipment, and networks.

For more details and assistance on how to protect your installation, please contact your local Schneider Electric Industrial Cybersecurity Services organization, which is fully aware of this situation and can support you through the process.

# Schneider Electric Security Notification

## Vulnerability Details

- [CVE-2020-11896](#)
- [CVE-2020-11897](#)
- [CVE-2020-11898](#)
- [CVE-2020-11899](#)
- [CVE-2020-11900](#)
- [CVE-2020-11901](#)
- [CVE-2020-11902](#)
- [CVE-2020-11903](#)
- [CVE-2020-11904](#)
- [CVE-2020-11905](#)
- [CVE-2020-11906](#)
- [CVE-2020-11907](#)
- [CVE-2020-11908](#)
- [CVE-2020-11909](#)
- [CVE-2020-11910](#)
- [CVE-2020-11911](#)
- [CVE-2020-11912](#)
- [CVE-2020-11913](#)
- [CVE-2020-11914](#)

Additional details on these specific vulnerabilities can be found on the ICS-CERT Advisory at <https://www.us-cert.gov/ics/advisories/ICSA-20-168-01>.

## 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 for the devices that it is intended for.
- 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.

## Schneider Electric Security Notification

### 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, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

<https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp>

For related information, refer to the Treck TCP/IP Vulnerabilities Security Bulletin:

<https://www.se.com/ww/en/download/document/SESB-2020-168-01>

#### Legal Disclaimer

THIS DOCUMENT IS 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 OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER 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. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

#### Revision Control:

<b>Version 1</b> 23 June 2020	Original Release
<b>Version 1.1</b> 24 June 2020	- Added link to related SEVD-2020-174-01 Security Notification document for Network Management Card (NMC) offers (pages 4-5) - Minor formatting changes
<b>Version 1.2</b> 27 June 2020	- Enhanced Andover Continuum affected product information (page 3) - Minor formatting changes
<b>Version 1.3</b> 2 July 2020	Added Acti9 Smartlink EL B to affected product list (page 2)
<b>Version 1.4</b> 14 July 2020	Removed Smartlink ELEC (duplicate reference for Acti9 Smartlink EL B ) from the affected product list (page 3)

## Schneider Electric Security Notification

<p><b>Version 2.0</b> 29 July 2020</p>	<ul style="list-style-type: none"> <li>- Added <i>Wiser Energy IP module by Schneider Electric</i>, <i>Wiser Energy IP module by Schneider Electric</i>, and <i>Gateway Connector by Elko</i> to affected products list (<a href="#">page 5</a>)</li> <li>- Added <i>XUPH001 OsSense communication module</i> and <i>XGCS850C201 OsiSense RFID compact smart antenna</i> to affected products list (<a href="#">page 2</a>)</li> <li>- Removed <i>PowerLogic EGX100</i>, <i>ECI850 Sepam IEC 61850 Server</i>, and <i>PowerLogic G3200 Modbus to IEC 61850 Gateway</i> from affected products list. (<a href="#">page 3</a>)</li> </ul>
<p><b>Version 2.1</b> 5 August 2020</p>	<p>Added remediation for <i>Uninterruptible Power Supply (UPS) using NMC2</i> (<a href="#">page 2</a>)</p>
<p><b>Version 2.2</b> 6 August 2020</p>	<p>Corrected affected version(s) and enhanced remediation/mitigation version details for <i>Uninterruptible Power Supply (UPS) using NMC2</i> (<a href="#">page 2</a>)</p>
<p><b>Version 2.3</b> 1 September 2020</p>	<p>Added remediation for <i>Cooling Products using NMC2</i> and partial remediations for <i>ATM3BC bus coupler module – EIP</i>, <i>TM3BC bus coupler module – SL</i>, and <i>TM3BC bus coupler module – CANOpen</i> (<a href="#">page 2-3</a>)</p>
<p><b>Version 2.4</b> 13 October 2020</p>	<p>Added remediation guidance for <i>VW3A3310 Altivar 61/71 Modbus TCP</i>, <i>VW3A3310D Altivar 61/71 Ethernet daisy chain</i>, <i>VW3A3316 Altivar 61/71 Ethernet IP</i>, and <i>VW3A3320 Altivar 61/71 Ethernet IP RSTP options</i>. (<a href="#">page 2-3</a>)</p>
<p><b>Version 2.5</b> 23 October 2020</p>	<ul style="list-style-type: none"> <li>- Added remediation for <i>EGX150/Link150 Ethernet Gateway</i>, <i>Acti9 PowerTag Link / HD</i>, <i>Acti9 Smartlink SI D</i>, and <i>Acti9 Smartlink SI B</i></li> <li>- All APC Network Management Card related impact and remediation information has been moved to the existing <a href="#">Security Notification SEVD-2020-174-01</a> for increased clarity.</li> <li>- Added <i>PowerLogic EGX100</i> to affected products list             <ul style="list-style-type: none"> <li>• <b>Note:</b> Based on information received earlier this year, Schneider Electric originally determined that its <i>PowerLogic EGX100</i> was not affected by vulnerabilities in Treck Inc.'s embedded TCP/IP stack. After receiving additional information and analysis from Treck, Inc and JSOF, Schneider Electric has determined this offer is impacted. Users of this product are encouraged to apply the <a href="#">recommended mitigation</a> actions immediately to minimize the risks associated with vulnerabilities in Treck Inc.'s embedded TCP/IP stack.</li> </ul> </li> </ul>
<p><b>Version 2.6</b> 10 November 2020</p>	<p>Added remediations for <i>eIFE Ethernet Interface for MasterPact MTZ drawout circuit breakers</i>, <i>IFE Ethernet Interface for ComPact</i>, <i>PowerPact</i>, and <i>MasterPact circuit breakers</i>, and <i>IFE Gateway</i> (<a href="#">page 4</a>)</p>

## Schneider Electric Security Notification

<p><b>Version 2.7</b> 8 December 2020</p>	<p>Added remediations for SCADAPack 32 RTU, XUPH001 OsSense communication module, XGCS850C201 OsiSense RFID compact smart antenna, ATV340E Altivar Machine Drives, ATV630/650/660/680/6A0/6B0 Altivar Process Drives, ATV930/950/960/980/9A0/9B0 Altivar Process Drives, VW3A3720, VW3A3721 Altivar Process Communication Modules, ACE850 Sepam communication interface, PowerLogic EGX300 Ethernet Gateway, PowerLogic EGX100 Ethernet Gateway, Acti9 Smartlink IP (page 2, 4-5)</p>
<p><b>Version 2.8</b> 18 December 2020</p>	<p>Added remediations for EcoStruxure Building SmartX IP RP Controllers and EcoStruxure Building SmartX IP MP Controllers (page 6)</p>