Schneider Electric Security Notification

EcoStruxure™ Control Expert, EcoStruxure™ Process Expert, SCADAPack RemoteConnect™ x70, and Modicon Controllers M580 and M340

13 July 2021

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure Control Expert, EcoStruxure Process Expert, SCADAPack RemoteConnect x70, and Modicon M580 and M340 control products. These vulnerabilities pose several risks, primary among these is the possibility of arbitrary code execution and loss of confidentiality and integrity of the project file.

With all products affected an attack would first involve an authenticated user gaining access to the engineering station; or an unauthenticated user gaining access to a project file or to the process control network.

Our findings demonstrate that while the discovered vulnerabilities affect Schneider Electric offers, it is possible to mitigate the potential impacts by following standard guidance, specific instructions; and in some cases, the fixes provided by Schneider Electric to remove the vulnerabilities.

Please ensure that if you are an EcoStruxure Control Expert user to apply the security updates released on July 12, 2021. For users of any of the mentioned products see the mitigation section in this security notice for further information on how to help protect your system from possible attack.

Schneider Electric encourages all industrial companies to ensure they have implemented cybersecurity best practices across their operations and supply chains to reduce cyber risks. Where appropriate this includes locating 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; systematically applying security patches.

Schneider Electric Security Notification

Affected Products

	CVE-					
	2021-22778	2021-22779	2021-22780	2021-22781	2021-22782	2020-12525
EcoStruxure Control Expert, all versions prior to V15.0 SP1 Including all versions of Unity Pro (former name of EcoStruxure Control Expert)	X	X	X	X	X	X
EcoStruxure Control Expert V15.0 SP1		X				X
EcoStruxure Process Expert, all versions Including all versions of EcoStruxure Hybrid DCS (former name of EcoStruxure Process Expert)	X	X	X	X	X	X
SCADAPack RemoteConnect for x70, all versions	X	X	X	X	X	X
Modicon M580 CPU (part numbers BMEP* and BMEH*), all versions		X				
Modicon M340 CPU (part numbers BMXP34*), all versions		X				

Vulnerability Details

CVE ID: **CVE-2021-22778**

CVSS v3.1 Base Score 8.6 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

A *CWE-522: Insufficiently Protected Credentials* vulnerability exists that could cause protected derived function blocks to be read or modified by unauthorized users when accessing a project file.

CVE ID: **CVE-2021-22779**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-290: Authentication Bypass by Spoofing* vulnerability exists that could cause unauthorized access in read and write mode to the controller by spoofing the Modbus communication between the engineering software and the controller.

Schneider Electric Security Notification

CVE ID: **CVE-2020-12525**

CVSS v3.1 Base Score 7.3 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

M&M Software fdtCONTAINER Component in versions below 3.5.20304.x and between 3.6 and 3.6.20304.x is vulnerable to deserialization of untrusted data in its project storage.
Note: This vulnerability could cause local code execution on the engineering workstation when a malicious project file is loaded into the engineering software.

CVE ID: **CVE-2021-22780**

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

A *CWE-522: Insufficiently Protected Credentials* vulnerability exists that could cause unauthorized access to a project file protected by a password when this file is shared with untrusted sources. An attacker may bypass the password protection and be able to view and modify a project file.

CVE ID: **CVE-2021-22781**

CVSS v3.1 Base Score 6.2 | Medium | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A *CWE-522: Insufficiently Protected Credentials* vulnerability exists that could cause a leak of SMTP credential used for mailbox authentication when an attacker can access a project file.

CVE ID: **CVE-2021-22782**

CVSS v3.1 Base Score 6.2 | Medium | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A *CWE-311: Missing Encryption of Sensitive Data* vulnerability exists that could cause an information leak allowing disclosure of network and process information, credentials or intellectual property when an attacker can access a project file.

Remediations & Mitigations

EcoStruxure Control Expert, versions prior to V15.0 SP1	**EcoStruxure Control Expert V15.0 SP1**, available for download below, includes a fix for:
	• CVE-2021-22778
	• CVE-2021-22780
	• CVE-2021-22781
	• CVE-2021-22782
	
	https://www.se.com/ww/en/download/document/EcoStruxureControlExpert_15SP1
	
	Important Note:
	• The fix is provided through the additional feature “file encryption”, for further information on the feature and how to set it up please refers to the chapter “file encryption” of the help file available in the EcoStruxure Control Expert v15.0 SP1.
	• This feature is proposed by default when creating a new project.
	• This feature is also available, after selecting “project” in structural view, in the “Edit/ Properties/ Project & Controller Protection” menu.
	• **For new projects:**
	  ○ Customers are recommended to apply this feature to all new projects.
	• **For existing projects:**
	  ○ Customers are recommended to apply this feature to the existing projects coming from trusted source. For .sta project files, as a reminder, project modification can be done in connected mode to prevent desynchronization and keep the controller in RUN state.
	• It is possible to set a security level specific to the Derived Function Blocks (DFB) in addition to the file encryption feature. Please refer to the chapter "How to protect a DFB type" in the EcoStruxure Control Expert help file for further information.
	• Customers are recommended to share project files only when configured with the encryption feature described above.
	
	We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure.
	
	Contact Schneider Electric’s Customer Care Center if you need assistance removing a patch. If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit.

EcoStruxure Control Expert, all versions Including all versions of Unity Pro (former name of EcoStruxure Control Expert)	Schneider Electric is establishing a remediation plan for the future versions that will include additional fixes for the above vulnerabilities. We will update this document when the remediations are available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Apply the remediation steps provided above to address the project file vulnerabilities • Use the new "file encryption" feature available on EcoStruxure Control Expert v15.0 SP1 For all versions of EcoStruxure Control Expert, including V15.0 SP1, the following mitigations apply for the remaining vulnerabilities • Store the project files in a secure storage and restrict the access to only trusted users • When exchanging files over the network, use secure communication protocols • Encrypt project files when stored • Only open project files received from trusted source • Compute a hash of the project files and regularly check the consistency of this hash to verify the integrity before usage • Harden the workstation running EcoStruxure Control Expert or Unity Pro Customers using Unity Pro should strongly consider migrating to EcoStruxure Control Expert. Please contact your local Schneider Electric technical support for more information. To ensure you are informed of all security notifications updates, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp
EcoStruxure Process Expert, all versions Including all versions of EcoStruxure Hybrid DCS (former name of EcoStruxure Process Expert)	Schneider Electric is establishing a remediation plan for future versions that will include additional fixes for the above vulnerabilities. We will update this document when the remediations are available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Store the project files in a secure storage and restrict the access to only trusted users • When exchanging files over the network, use secure communication protocols • Encrypt project files when stored • Only open project files received from trusted source • Compute a hash of the project files and regularly check the consistency of this hash to verify the integrity before usage • Harden the workstation running EcoStruxure Process Expert To ensure you are informed of all security notifications updates, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

SCADAPack RemoteConnect, all versions	Schneider Electric is establishing a remediation plan for the future versions that will include additional fixes for the above vulnerabilities. We will update this document when the fixes are available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Store the project files in a secure storage and restrict the access to only trusted users • When exchanging files over the network, use secure communication protocols • Encrypt project files when stored • Only open project files received from trusted source • Compute a hash of the project files and regularly check the consistency of this hash to verify the integrity before usage • Harden the workstation running SCADAPack RemoteConnect
Modicon M580 CPU (part numbers BMEP* and BMEH*), all versions	To mitigate the authentication bypass vulnerability between the engineering workstation and the controller (**CVE-2021-22779**), additional hardening measures are needed on the controller side to reduce the risk of exploit: **Modicon M580:** • Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP • Configure the Access Control List following the recommendations of the user manual “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 BMENOC module and follow the instructions to configure IPSEC feature as described in the guideline “Modicon M580 - BMENOC03.1 Ethernet Communications Schneider Electric Security Notification Module, Installation and Configuration Guide” in the chapter “Configuring IPSEC communications”: https://www.se.com/ww/en/download/document/HRB62665/ • Setup a VPN between the Modicon PLC impacted modules and the engineering workstation containing EcoStruxure Control Expert or Process Expert.

Modicon M340 CPU (part numbers BMXP34*), all versions	To mitigate the authentication bypass vulnerability (**CVE-2021-22779**) between the engineering workstation and the controller, additional hardening measures are needed on the controller side to reduce the risk of exploit: **Modicon M340:** • Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP • Configure the Access Control List following the recommendations of the user manual "Modicon M340 for Ethernet Communications Modules and Processors User Manual" in chapter "Messaging Configuration Parameters": https://www.se.com/ww/en/download/document/31007131K01000/ • Setup a VPN between the Modicon PLC impacted modules and the engineering workstation containing EcoStruxure Control Expert or Process Expert.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Ensure the cybersecurity features in Schneider Electric solutions are always enabled.
- 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 when applicable do not leave them in the "Program" mode.
- Never connect programming software and engineering workstations to any network other than the network that it is intended.
- ICS networks should be appropriately partitioned, and not directly connected to business networks or the Internet.
- 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.

- Customers are encouraged to implement best practices covered in the Top 20 Secure PLC Coding Practices to help improve the security posture of their Industrial Control Systems.

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

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to this vulnerabilities:

CVE	Researchers
CVE-2021-22779	• Kai Wang (Fortinet's FortiGuard Labs) • Nicholas Miles (Tenable) • Andrey Muravitsky (Kaspersky ICS CERT) • Gal Kauffman (Armis) • Li Wei (Friday Lab - Bolean Tech)
CVE-2021-22780	• Kai Wang (Fortinet's FortiGuard Labs) • Maxim Tumakov (Kaspersky ICS CERT)
CVE-2021-22781	• Kai Wang (Codesafe Team of Legendsec at Qi'anxin Group)
CVE-2021-22782	• Maxim Tumakov (Kaspersky ICS CERT)

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. 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

Schneider Electric Security Notification

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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *13 Jul 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.07.13 07:27:13 -04'00'