Schneider Electric Security Notification

EcoStruxure™ and SmartStruxure™
Power Monitoring and SCADA Software

13 October 2020

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ and SmartStruxure™ Power Monitoring & SCADA Software.

Failure to apply the mitigation provided below may risk remote code execution, which could result in an attacker gaining root level access to the underlying operating system on the impacted server.

Affected Product and Version

EcoStruxure™ Power Monitoring Expert versions 9.0, 8.x, 7.x
EcoStruxure™ Energy Expert version 2.0
Power Manager versions 1.1, 1.2, 1.3
StruxureWare™ PowerSCADA Expert with Advanced Reporting and Dashboards Module versions 8.x
EcoStruxure™ Power SCADA Operation with Advanced Reporting and Dashboards Module version 9.0

Vulnerability Details

CVE ID: **CVE-2020-7545**

CVSS v3.0 Base Score 8.4 | High | CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H

A CWE-284:Improper Access Control vulnerability exists that could allow for arbitrary code execution on the server when an authorized user access an affected webpage.

CVE ID: **CVE-2020-7546**

CVSS v3.0 Base Score 5.4 | Medium | CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

A CWE-79: Improper Neutralization of Input During Web Page Generation vulnerability exists that could allow an attacker to perform actions on behalf of the authorized user when accessing an affected webpage.

CVE ID: **CVE-2020-7547**

CVSS v3.0 Base Score 6.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

A CWE-284: Improper Access Control vulnerability exists that could allow a user the ability to perform actions via the web interface at a higher privilege level.

Remediation

Affected Product & Version	Remediation
Power Monitoring Expert Versions 9.0, 8.x, 7.x	These vulnerabilities have been fixed in **EcoStruxure™ Power Monitoring Expert Version 2020**, contact your Schneider Electric representative for details on how to upgrade your system.
Energy Expert Version 2.0	These vulnerabilities have been fixed in **EcoStruxure™ Energy Expert V3.0**, contact your Schneider Electric representative for details on how to upgrade your system.
Power Manager Versions 1.1, 1.2, 1.3	Contact customer support for mitigation instructions, or your Schneider Electric representative for details on how to upgrade your system.
PowerSCADA Expert with Advanced Reporting and Dashboards Module Versions 8.x	Contact customer support for mitigation instructions, or your Schneider Electric representative for details on how to upgrade your system.
Power SCADA Operation with Advanced Reporting and Dashboards Module Version 9.0	These vulnerabilities have been fixed in **EcoStruxure™ Power SCADA Operations with Advanced Reporting and Dashboard Module Products version 2020**., contact your Schneider Electric representative for details on how to upgrade your system.

If customers choose not to apply the remediation provided above, they should immediately contact customer support for mitigation instructions to reduce the risk of exploit.

Customers should use appropriate patching methodologies when applying these patches to their systems. 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.

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.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2020-7545	Michiel Evers and Niels Pirotte
CVE-2020-7546, CVE-2020-7547	Michiel Evers

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

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

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 *13 October 2020*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2020.10.11 17:05:25 -04'00'