Schneider Electric Security Notification

EcoStruxure Geo SCADA Expert

8 December 2020

Overview

Schneider Electric is aware of a vulnerability in the Schneider Electric EcoStruxure Geo SCADA Expert product.

EcoStruxure Geo SCADA Expert software is an integrated, scalable and reliable Supervisory Control and Data Acquisition (SCADA) software with ready-to-use telemetry features optimized for managing remote assets spread across geographically dispersed infrastructure.

Failure to apply the remediations provided below may risk the revealing of account credentials, which could result in unauthorized system access.

Affected Products & Versions

Product	Version
EcoStruxure Geo SCADA Expert 2019	Original release and Monthly Updates to September 2020, from 81.7268.1 to 81.7578.1
EcoStruxure Geo SCADA Expert 2020	Original release and Monthly Updates to September 2020, from 83.7551.1 to 83.7578.1

Vulnerability Details

CVE ID: **CVE-2020-28219**

CVSS v3.0 Base Score 6.5 | Medium | CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H

A CWE-522: Insufficiently Protected Credentials vulnerability exists that could cause exposure of credentials to server-side users when web users are logged in to Virtual ViewX.

Remediation

Product	Remediation
EcoStruxure Geo SCADA Expert 2019	The Monthly Updates from October 2020, 81.7613.1 include a fix for this vulnerability. Software is available for download here: https://tprojects.schneider-electric.com/telemetry/display/CS/Geo+SCADA+Expert+Downloads

EcoStruxure Geo SCADA Expert 2020	The Monthly Updates from October 2020, 83.7613.1 include a fix for this vulnerability. Software is available for download here: https://tprojects.schneider-electric.com/telemetry/display/CS/Geo+SCADA+Expert+Downloads

If Virtual ViewX is on a separate server from the Geo SCADA Server, then only Virtual ViewX software requires installation, although it is recommended to keep both up to date. If on the same server as the Geo SCADA Server then both components require update. Software updates may require reboots as requested.

This software update makes changes to the Virtual ViewX settings which can be performed manually. To do this and verify that the settings are in place, refer to the mitigation steps below.

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.

The steps to remediate this vulnerability are automatically applied by the October Monthly Updates. If customers choose not to update to the latest software, they should immediately follow these steps:

1. From the Virtual ViewX Manager app, select the 'Applications' tab.
2. Double-click the Virtual ViewX application in the list.
3. Then uncheck the setting 'Allow Browser Arguments'.
4. Finally click OK, then Apply and Close.

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.

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.

Schneider Electric Security Notification

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 *8 December 2020*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2020.12.06 14:09:37 -05'00'