Schneider Electric Security Notification

EcoStruxure Geo SCADA Expert (ClearSCADA) (V1.1)

10 December 2019 (15 April 2021)

Overview

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

Affected Products

EcoStruxure Geo SCADA Expert (ClearSCADA) with initial releases before 1 January 2019
This includes the following versions in current support:

- ClearSCADA 2017 R3
- ClearSCADA 2017 R2
- ClearSCADA 2017

Vulnerability Details

CVE ID: **CVE-2019-6854**

CVSS v3.0 Base Score 7.8 | (High) | AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A CWE-287: Improper Authentication vulnerability exists in a folder within EcoStruxure Geo SCADA Expert which could cause a low privilege user to delete or modify database, setting or certificate files. Those users must have access to the file system of that operating system to exploit this vulnerability.

Remediation

This vulnerability is fixed in version EcoStruxure Geo SCADA Expert 2019 and is available for download below:

https://tprojects.schneider-electric.com/telemetry/display/CS/ClearSCADA+Downloads

The following workarounds and mitigations can be applied by customers to reduce the risk:

- The vulnerability is addressed when the server and client applications create the program data directory structure when initially executed.

Schneider Electric Security Notification

For existing installations of ClearSCADA, and any upgraded installations of ClearSCADA, system administrators must set the correct file permissions for their 'ProgramData\Schneider Electric\...' folders.

The Application with older product versions (indicated by the ClearSCADA product name) will not be modified. Any modification to correct file permissions could, inappropriately, overwrite customer's own settings.

The following system changes can be applied by customers:

- The ACLs of the affected files should have permissions for the "Everyone" group removed, and instead, the files and directories should have ACLs added only for the users and groups that should be permitted to modify them (e.g., LocalSystem and Administrators).
- The ACLs can be adjusted during operation and there is no requirement for reboot, though we recommend that if you have redundant servers you make the changes separately and test them .

Product Information

EcoStruxure™ Geo SCADA Expert (formerly known as ClearSCADA) is an open, flexible and scalable software for telemetry and remote SCADA solutions

Product Category - Industrial Automation Control

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

a) Check your version of Geo SCADA Expert (ClearSCADA) in the About box of applications or the header of log files. It is of the form mm.bbbb. If the version mm is 80 or less, then the applications may initially create the `'ProgramData\Schneider Electric\...'` folders with permissions for the "Everyone" group.
b) Check file access permissions of the `'ProgramData\Schneider Electric\...'` folders. If the "Everyone" group has access then the system may be affected.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.

- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or 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), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is 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-2019-6854	William Knowles (Lancaster University)

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.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

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.

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 *10 December 2019*	Original Release
Version 1.1 15 April 2021	Updated CWE for CVE-2019-6854

Product Security Office

Digitally signed by Product Security Office
Date: 2021.04.15 17:05:01 -04'00'