Schneider Electric Security Notification

EcoStruxure™ Geo SCADA Expert

10 January 2023 (14 March 2023)

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Geo SCADA Expert software product, formerly known as ClearSCADA.

The EcoStruxure™ Geo SCADA Expert product is an open, flexible and scalable software for telemetry and remote SCADA solutions.

If successfully exploited, bad actors could execute a range of actions, including accessing and disclosing sensitive information, and denial of service.

Failure to apply the remediations provided below may risk unauthorized system access, which could result in SCADA configuration data being exposed or a loss of service.

March 2023 update: Adjustment of the deprecated CWE of the CVE-2023-22610.

Affected Products and Versions

Product	Version
EcoStruxure™ Geo SCADA Expert *2019* EcoStruxure™ Geo SCADA Expert *2020* EcoStruxure™ Geo SCADA Expert *2021* (formerly known as ClearSCADA)	All Versions prior to October 2022

Vulnerability Details

CVE ID: **CVE-2023-22610**

CVSS v3.1 Base Score 9.1 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

A *CWE-863: Incorrect Authorization* vulnerability exists that could cause Denial of Service against the Geo SCADA server when specific messages are sent to the server over the database server TCP port.

CVE ID: **CVE-2023-22611**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A *CWE-200: Exposure of Sensitive Information to an Unauthorized Actor* vulnerability exists that could cause information disclosure when specific messages are sent to the server over the database server TCP port.

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Geo SCADA Expert *2019* **EcoStruxure™ Geo SCADA Expert *2020*** **EcoStruxure™ Geo SCADA Expert *2021*** **ClearSCADA** *(previous product name)*	The October 2022 Updates of EcoStruxure™ Geo SCADA Expert include fixes for these vulnerabilities and are available for download here: https://community.se.com/t5/Geo-SCADA-Knowledge-Base/Geo-SCADA-Expert-Downloads/ba-p/279115 Installation of new server software will require a system restart or changeover of redundant servers. Consult the Release Notes and Exchange Knowledge Base (Resource Center) for advice on the procedure: https://community.exchange.se.com/t5/Geo-SCADA-Knowledge-Base/Resource-Center-Home/ba-p/279133 The documentation also states how to verify the installed version.

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.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit.

Mitigations

Affected Product & Version	Mitigations
EcoStruxure™ Geo SCADA Expert *2019* **EcoStruxure™ Geo SCADA Expert *2020*** **EcoStruxure™ Geo SCADA Expert *2021*** **ClearSCADA** *(the previous product name)*	To mitigate these vulnerabilities, we recommend restricting access to the Geo SCADA server's database port (default 5481). Access should be available only to ViewX clients. Refer to the Geo SCADA Expert Help documentation for advice and best practices for putting networks and remote devices behind firewalls and isolating them from the business network and public networks. Specific advice is listed below: • To protect client/server communications we recommend using the features in Geo SCADA Expert 2021 which perform server-side checks of client certificates. This feature helps protect against unknown clients connecting to the server. • Disable the setting "Allow guest user to execute SQL" if it is enabled.

	• Configure the Client Access Control list, which prevents unauthorized IP addresses from connecting. Also, you can use this to restrict access to Geo SCADA Server's web services port(s) (default 443). We recommend upgrading to the software versions listed in the section above. Customers using ClearSCADA should also upgrade to the latest GeoSCADA release.

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here:

https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

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 intended for that device.
- 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

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2023-22610 CVE-2023-22611	The UK's National Cyber Security Centre (NCSC)

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: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

Schneider Electric Security Notification

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 *10 January 2023*	Original Release
Version 1.1 *14 March 2023*	Adjustment of the deprecated CWE of the CVE-2023-22610.

Product Security Office

Digitally signed by Product Security Office
Date: 2023.03.13 15:09:07 -04'00'