

Schneider Electric Security Notification

EcoStruxure Geo SCADA Expert

08 February 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure Geo SCADA Expert product (formerly known as ClearSCADA).

[EcoStruxure Geo SCADA Expert](#) software is an open, flexible, and scalable software system for telemetry and remote SCADA solutions.

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

Affected Products and Versions

- ClearSCADA all versions
- EcoStruxure Geo SCADA Expert 2019, all versions
- EcoStruxure Geo SCADA Expert 2020, all versions

Vulnerability Details

CVE ID: **CVE-2022-24318**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L

A *CWE-326: Inadequate Encryption Strength* vulnerability exists that could cause non-encrypted communication with the server when outdated versions of the ViewX client are used.

CVE ID: **CVE-2022-24319**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L

A *CWE-295: Improper Certificate Validation* vulnerability exists that could allow a Man-in-the-Middle attack when communications between the client and Geo SCADA web server are intercepted.

CVE ID: **CVE-2022-24320**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L

A *CWE-295: Improper Certificate Validation* vulnerability exists that could allow a Man-in-the-Middle attack when communications between the client and Geo SCADA database server are intercepted.

CVE ID: **CVE-2022-24321**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists that could cause Denial of Service against the Geo SCADA server when receiving a malformed HTTP request.

Schneider Electric Security Notification

Remediation

The Geo SCADA Expert 2021 product includes fixes for all the above vulnerabilities and is available for download here:

<https://community.exchange.se.com/t5/Geo-SCADA-Knowledge-Base/Geo-SCADA-Expert-Downloads/ba-p/279115>

The following table details the CVEs that have also been fixed in earlier versions of Geo SCADA Expert.

CVE	Fixed Version
CVE-2022-24318	<ul style="list-style-type: none"> EcoStruxure Geo SCADA Expert 2021. All versions (84.*)
CVE-2022-24319	<ul style="list-style-type: none"> EcoStruxure Geo SCADA Expert 2021. All versions (84.*)
CVE-2022-24320	<ul style="list-style-type: none"> EcoStruxure Geo SCADA Expert 2021. All versions (84.*) EcoStruxure Geo SCADA Expert 2020, October 2021 Monthly Update. (83.7980.2)
CVE-2022-24321	<ul style="list-style-type: none"> EcoStruxure Geo SCADA Expert 2021. All versions (84.*) EcoStruxure Geo SCADA Expert 2020, August 2021 Monthly Update. (83.7913.1) EcoStruxure Geo SCADA Expert 2019, August 2021 Monthly Update. (81.7896.1) ClearSCADA 2017 R3 August 2021 Monthly Update. (80.7896.1)

Installation of new server software will require 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>

Please read the product documentation to understand how to set up client and server certificates and how to configure connections to restrict to client versions supporting certificates.

Customers should use appropriate update methodologies when applying these updates to their systems. We strongly recommend the use of back-ups and evaluating the impact of these updates in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's [Customer Care Center](#) if you need assistance removing an update.

We recommend upgrading to the latest software versions listed in the section above. If customers choose not to apply the remediations provided above, they should immediately apply the general security recommendations and the following mitigations to reduce the risk of exploit:

Schneider Electric Security Notification

Restrict access to the Geo SCADA server's database port (default 5481/TCP) and Geo SCADA Server's web services port (default 443/TCP). Access should be available only to ViewX and WebX client.

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.

Acknowledgements

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

CVE	Researchers
CVE-2022-24318 CVE-2022-24321	Frank Lycops (Asvalis)
CVE-2022-24319 CVE-2022-24320	Frank Lycops (Asvalis) Cameron Stokes (Mandiant)

Schneider Electric Security Notification

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>

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:

<p>Version 1.0 <i>08 Feb 2022</i></p>	<p>Original Release</p>
--	-------------------------