

Schneider Electric Security Notification

EcoStruxure™ Geo SCADA Expert

14 February 2023

Overview

Schneider Electric is aware of a vulnerability 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 arbitrarily inject text entries into product log files, including falsified entries, or filling the log files with bad data.

Failure to apply the remediation provided below may risk the compromise of product log files.

Affected Products and Versions

Product	Version
EcoStruxure™ Geo SCADA Expert 2019, EcoStruxure™ Geo SCADA Expert 2020, EcoStruxure™ Geo SCADA Expert 2021	All Versions prior to October 2022
ClearSCADA	All Versions

Vulnerability Details

CVE ID: **CVE-2023-0595**

CVSS v3.1 Base Score 5.3 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

A *CWE-117: Improper Output Neutralization for Logs* vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443).

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
<p>EcoStruxure™ Geo SCADA Expert 2019, EcoStruxure™ Geo SCADA Expert 2020, EcoStruxure™ Geo SCADA Expert 2021 <i>All Versions prior to October 2022</i></p> <p>ClearSCADA <i>(previous product name)</i> <i>All Versions</i></p>	<p>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</p> <p>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</p> <p>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.</p> <p>The documentation also states how to verify the installed version.</p>

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
<p>EcoStruxure™ Geo SCADA Expert 2019, EcoStruxure™ Geo SCADA Expert 2020, EcoStruxure™ Geo SCADA Expert 2021 <i>All Versions prior to October 2022</i></p> <p>ClearSCADA <i>(previous product name)</i> <i>All Versions</i></p>	<p>To mitigate these vulnerabilities, we recommend restricting access to the Geo SCADA server's database web port (default 443). Access should be available only to ViewX and WebX clients.</p> <p>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:</p> <ul style="list-style-type: none"> • Configure the Geo SCADA Server's Client Access Control list, which prevents unauthorized IP addresses from connecting. <p>We recommend upgrading to the software versions listed in the section above. Customers using ClearSCADA should also upgrade.</p>

Schneider Electric Security Notification

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.

Acknowledgements

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

CVE	Researcher
CVE-2023-0595	Frank Lycops (Asvalis)

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

Schneider Electric Security Notification

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

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.

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:

<p>Version 1.0 14 February 2023</p>	<p>Original Release</p>
--	-------------------------