

Schneider Electric Security Notification

IGSS (Interactive Graphical SCADA System)

08 February 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in the IGSS (Interactive Graphical SCADA System) Data Server module.

The [IGSS](#) product is a state-of-the art SCADA system used for monitoring and controlling industrial processes. The Data Server is a module with a TCP interface used by other modules to access data of the SCADA System.

Failure to apply the remediations provided below may risk remote code execution, which could result in a variety of issues including disclosure of data and loss of control of the SCADA System with IGSS running in production mode.

Affected Product and Versions

Product	Version
IGSS Data Server (IGSSdataServer.exe)	V15.0.0.22020 and prior

Vulnerability Details

CVE ID: **CVE-2022-24310**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-190: Integer Overflow or Wraparound* vulnerability exists that could cause heap-based buffer overflow, leading to denial of service and potentially remote code execution when an attacker sends multiple specially crafted messages.

CVE ID: **CVE-2022-24311**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory* vulnerability exists that could cause modification of an existing file by inserting at beginning of file or create a new file in the context of the Data Server potentially leading to remote code execution when an attacker sends a specially crafted message.

Schneider Electric Security Notification

CVE ID: **CVE-2022-24312**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory* vulnerability exists that could cause modification of an existing file by adding at end of file or create a new file in the context of the Data Server potentially leading to remote code execution when an attacker sends a specially crafted message.

CVE ID: **CVE-2022-24313**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-120: Buffer Copy without Checking Size of Input* vulnerability exists that could cause a stack-based buffer overflow potentially leading to remote code execution when an attacker sends a specially crafted message.

CVE ID: **CVE-2022-24314**

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

A *CWE-125: Out-of-bounds Read* vulnerability exists that could cause memory leaks potentially resulting in denial of service when an attacker repeatedly sends a specially crafted message.

CVE ID: **CVE-2022-24315**

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

A *CWE-125: Out-of-bounds Read* vulnerability exists that could cause denial of service when an attacker repeatedly sends a specially crafted message.

CVE ID: **CVE-2022-24316**

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

A *CWE-665: Improper Initialization* vulnerability exists that could cause information exposure when an attacker sends a specially crafted message.

CVE ID: **CVE-2022-24317**

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

A *CWE-862: Missing Authorization* vulnerability exists that could cause information exposure when an attacker sends a specific message.

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
IGSS Data Server V15.0.0.22020 and prior	Version 15.0.0.22021 of IGSS Data Server includes corrections for these vulnerabilities and is available for download through IGSS Master > Update IGSS Software or here: https://igss.schneider-electric.com/igss/igssupdates/v150/IGSSUPDATE.ZIP

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:

- Follow the general security recommendations below and verify that devices are isolated on a private network and that firewalls are configured with strict boundaries for devices that require remote access.

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.

Schneider Electric Security Notification

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 this vulnerability:

CVE	Researchers
CVE-2022-24310, CVE-2022-24314	Tenable
CVE-2022-24311, CVE-2022-24312, CVE-2022-24313, CVE-2022-24315, CVE-2022-24316, CVE-2022-24317	Vyacheslav Moskvina working with Trend Micro Zero Day Initiative

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

Schneider Electric Security Notification

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:

Version 1.0 <i>08 February 2022</i>	Original Release
---	-------------------------