Schneider Electric Security Notification

IGSS (Interactive Graphical SCADA System)

14 June 2022 (14 March 2023)

Overview

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

IGSS product is a 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 remediation provided below may result in denial of service and data files in the IGSS Report folder being lost, added, changed, or exposed. Further, it may risk remote code execution, which could result in various issues, including disclosure of data and loss of control of the SCADA System with IGSS running in production mode.

March 14, 2023 Update: The CVE-2022-32528 description details have been clarified (page 2).

Affected Product and Version

Product	Version
IGSS Data Server (IGSSdataServer.exe)	V15.0.0.22170 and prior

Vulnerability Details

CVE ID: **CVE-2022-32522**

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 specially crafted mathematically reduced data request messages.

CVE ID: **CVE-2022-32523**

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 specially crafted online data request messages.

CVE ID: **CVE-2022-32524**

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 specially crafted time reduced data messages.

CVE ID: **CVE-2022-32525**

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 specially crafted alarm data messages.

CVE ID: **CVE-2022-32526**

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 specially crafted setting value messages.

CVE ID: **CVE-2022-32527**

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 specially crafted alarm cache data messages.

CVE ID: **CVE-2022-32529**

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 specially crafted log data request messages.

CVE ID: **CVE-2022-32528**

CVSS v3.1 Base Score 8.6 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

A *CWE-306: Missing Authentication for Critical Function* vulnerability exists that could cause access to manipulate and read specific files in the IGSS project report directory, potentially leading to a denial-of-service condition when an attacker sends specific messages.

Remediation

Affected Product & Version	Remediation
IGSS Data Server *V15.0.0.22170 and prior*	V15.0.0.22171 of IGSS Data Server includes a fix for these vulnerabilities and is available for download through IGSS Master > Update IGSS Software or here: Online IGSS Updates Page: https://igss.schneider-electric.com/licensed-versions/ Direct Download: 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 recommendation 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.

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-2022-32528	Tenable
CVE-2022-32522, CVE-2022-32523, CVE-2022-32524, CVE-2022-32525, CVE-2022-32526, CVE-2022-32527, CVE-2022-32529	ADLab of Venustech & Tenable

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

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:

Version 1.0 *14 June 2022*	Original Release
Version 2.0 *23 June 2022*	The affected versions have been updated to include versions up to V15.0.0.22170.
Version 2.1 *14 March 2023*	The CVE-2022-32528 description details have been clarified (page 2).

Product Security Office

Digitally signed by Product Security Office
Date: 2023.03.13 15:07:05 -04'00'