Schneider Electric Security Notification

IGSS (Interactive Graphical SCADA System)

14 March 2023

Overview

Schneider Electric is aware of multiple vulnerabilities in its Data Server, Dashboard and Custom Reports modules for the IGSS (Interactive Graphical SCADA System) product.

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 like the Dashboard and the Custom Reports to access data of the SCADA System to be presented.

Failure to apply the remediation provided below may result in Denial of Service and dashboards or report files in the IGSS Report folder being lost, added or changed. Further it may risk remote code execution, which could result in a variety of issues including loss of control of the SCADA System with IGSS running in production mode.

Affected Products and Versions

Product	Version
IGSS Data Server (IGSSdataServer.exe)	V16.0.0.23040 and prior
IGSS Dashboard (DashBoard.exe)	V16.0.0.23040 and prior
Custom Reports (RMS16.dll)	V16.0.0.23040 and prior

Vulnerability Details

CVE ID: **CVE-2023-27980**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-306: Missing Authentication for Critical Function* vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report.

CVE ID: **CVE-2023-27982**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-345: Insufficient Verification of Data Authenticity* vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file.

CVE ID: **CVE-2023-27978**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-502: Deserialization of Untrusted Data* vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file.

CVE ID: **CVE-2023-27981**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory* vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report.

CVE ID: **CVE-2023-27984**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-20: Improper Input Validation* vulnerability exists in Custom Reports that could cause a macro to be executed, potentially leading to remote code execution when a user opens a malicious report file planted by an attacker.

CVE ID: **CVE-2023-27977**

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

A *CWE-345: Insufficient Verification of Data Authenticity* vulnerability exists in the Data Server that could cause access to delete files in the IGSS project report directory, this could lead to loss of data when an attacker sends specific crafted messages to the Data Server TCP port.

CVE ID: **CVE-2023-27979**

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

A *CWE-345: Insufficient Verification of Data Authenticity* vulnerability exists in the Data Server that could allow the renaming of files in the IGSS project report directory, this could lead to denial of service when an attacker sends specific crafted messages to the Data Server TCP port.

CVE ID: **CVE-2023-27983**

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

A *CWE-306: Missing Authentication for Critical Function* vulnerability exists in the Data Server TCP interface that could allow deletion of reports from the IGSS project report directory, this would lead to loss of data when an attacker abuses this functionality.

Remediation

Affected Product & Version	Remediation
IGSS Data Server **IGSS Dashboard** **IGSS Custom Reports** *V16.0.0.23040 and prior*	Version 16.0.0.23041 of IGSS Data Server, Dashboard and Custom Reports (RMS) includes corrections and mitigations for these vulnerabilities and is available for download through IGSS Master > Update IGSS Software or here: https://igss.schneider-electric.com/igss/igssupdates/v160/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:

- Read the Security Guideline for IGSS on securing an IGSS SCADA-installation.
- Make sure to take backup of files in the report directory. In the System Configuration module under Files, automatic backup can be enabled for the file types to backup.
- Strip report output from Excel output. In the System Configuration module under Reports, stripping of macros for the output engine can be enabled, reducing the risk of distributing an unsafe report.
- 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.

Note: Since the IGSS Custom Reports rely on Excel, customers should avoid using report formats in the xlsm format that can potentially contain malicious macros. Before opening an xlsm report format file from IGSS Master, users will now have to confirm that input is trusted, like what Excel does when an Excel workbook with macros is opened.

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 these vulnerabilities:

CVE	Researcher
CVE-2023-27977 CVE-2023-27978 CVE-2023-27979 CVE-2023-27980 CVE-2023-27981 CVE-2023-27982 CVE-2023-27983 CVE-2023-27984	kimiya 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

Schneider Electric Security Notification

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 March 2023*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2023.03.13 15:12:35 -04'00'