Schneider Electric Security Notification

IGSS (Interactive Graphical SCADA System)

8 June 2021

Overview

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

The IGSS product is a state-of-the art SCADA system used for monitoring and controlling industrial processes. IGSS communicates with all major industry standard PLC drivers.

Failure to apply the remediations provided below may risk remote code execution, which could result in an attacker gaining access to the Windows Operating System on the machine used to import CGF and WSP files, typically a step performed during system design time.

Affected Product and Versions

CVE	Product and Versions
CVE-2021-22750	IGSS Definition (Def.exe) V15.0.0.21041 and prior
CVE-2021-22751	IGSS Definition (Def.exe) V15.0.0.21140 and prior
CVE-2021-22752	
CVE-2021-22753	
CVE-2021-22754	
CVE-2021-22755	
CVE-2021-22756	
CVE-2021-22757	
CVE-2021-22758	
CVE-2021-22759	
CVE-2021-22760	
CVE-2021-22761	
CVE-2021-22762	

Vulnerability Details

CVE ID: **CVE-2021-22750**

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-787: Out-of-bounds write* vulnerability exists that could result in loss of data or remote code execution due to missing length checks, when a malicious CGF file is imported to IGSS Definition.

Schneider Electric Security Notification

CVE ID: **CVE-2021-22751**

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-787: Out-of-bounds write* vulnerability exists that could result in disclosure of information or execution of arbitrary code due to lack of input validation, when a malicious CGF (Configuration Group File) file is imported to IGSS Definition.

CVE ID: **CVE-2021-22752**

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-787: Out-of-bounds write* vulnerability exists that could result in loss of data or remote code execution due to missing size checks, when a malicious WSP (Workspace) file is being parsed by IGSS Definition.

CVE ID: **CVE-2021-22753**

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-125: Out-of-bounds read* vulnerability exists that could result in loss of data or remote code execution due to missing length checks, when a malicious WSP file is being parsed by IGSS Definition.

CVE ID: **CVE-2021-22754**

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-787: Out-of-bounds write* vulnerability exists that could result in loss of data or remote code execution due to lack of proper validation of user-supplied data, when a malicious CGF file is imported to IGSS Definition.

CVE ID: **CVE-2021-22755**

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-787: Out-of-bounds write* vulnerability exists that could result in disclosure of information or remote code execution due to lack of sanity checks on user-supplied data, when a malicious CGF file is imported to IGSS Definition.

CVE ID: **CVE-2021-22756**

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-125: Out-of-bounds read* vulnerability exists that could result in disclosure of information or remote code execution due to lack of user-supplied data validation, when a malicious CGF file is imported to IGSS Definition.

CVE ID: **CVE-2021-22757**

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-125: Out-of-bounds read* vulnerability exists that could result in disclosure of information or remote code execution due to lack of sanity checks on user-supplied input data, when a malicious CGF file is imported to IGSS Definition.

CVE ID: **CVE-2021-22758**

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-824: Access of uninitialized pointer* vulnerability exists that could result in loss of data or remote code execution due to lack validation of user-supplied input data, when a malicious CGF file is imported to IGSS Definition.

CVE ID: **CVE-2021-22759**

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-416: Use after free* vulnerability exists that could result in loss of data or remote code execution due to use of unchecked input data, when a malicious CGF file is imported to IGSS Definition.

CVE ID: **CVE-2021-22760**

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-763: Release of invalid pointer or reference* vulnerability exists that could result in loss of data or remote code execution due to missing checks of user-supplied input data, when a malicious CGF file is imported to IGSS Definition.

CVE ID: **CVE-2021-22761**

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer* vulnerability exists that could result in disclosure of information or remote code execution due to missing length check on user supplied data, when a malicious CGF file is imported to IGSS Definition.

CVE ID: **CVE-2021-22762**

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* exists that could result in remote code execution, when a malicious CGF or WSP file is being parsed by IGSS Definition.

Remediation

Version 15.0.0.21141 of the IGSS Definition module: Def.exe includes fixes 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:

- Avoid importing CGF and WSP files from untrusted sources.

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 for the devices that it is intended for.
- 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 this vulnerability:

CVE	Researchers
CVE-2021-22751, CVE-2021-22752, CVE-2021-22753, CVE-2021-22754, CVE-2021-22755, CVE-2021-22756, CVE-2021-22757, CVE-2021-22758, CVE-2021-22759, CVE-2021-22760	Michael Heinzl
CVE-2021-22750, CVE-2021-22752, CVE-2021-22753, CVE-2021-22761, CVE-2021-22762	kimiya working with Trend Micro's 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 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 *8 June 2021*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2021.06.06 20:16:01 -04'00'