Schneider Electric Security Notification

IGSS (Interactive Graphical SCADA System)

9 March 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 files, typically a step performed during system design time.

Affected Product and Versions

IGSS Definition (Def.exe) version 15.0.0.21041 and prior

Vulnerability Details

CVE ID: **CVE-2021-22709**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/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 loss of data or remote code execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.

CVE ID: **CVE-2021-22710**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/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 cause remote code execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition.

CVE ID: **CVE-2021-22711**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/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 arbitrary read or write conditions when malicious CGF (Configuration Group File) file is imported to IGSS Definition due to missing validation of input data.

Schneider Electric Security Notification

CVE ID: **CVE-2021-22712**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/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 arbitrary read or write conditions when malicious CGF (Configuration Group File) file is imported to IGSS Definition due to an unchecked pointer address.

Remediation

Version 15.0.0.21042 of the IGSS Definition module: Def.exe includes a fix for each of 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 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.

Schneider Electric Security Notification

- 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-2021-22709, CVE-2021-22710, CVE-2021-22711, CVE-2021-22712	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

Schneider Electric Security Notification

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 9 March 2021	Original Release