Schneider Electric Security Notification

IGSS (Interactive Graphical SCADA System)

12 October 2021

Overview

Schneider Electric is aware of multiple vulnerabilities in its Data Collector module for IGSS (Interactive Graphical SCADA System) 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 in worst case could result in an attacker gaining access to the Windows Operating System on the machine running IGSS in production.

Affected Product and Versions

IGSS Data Collector (dc.exe) V15.0.0.21243 and prior

Vulnerability Details

CVE ID: **CVE-2021-22802**

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 result in remote code execution due to missing length check on user supplied data, when a constructed message is received on the network.

CVE ID: **CVE-2021-22803**

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-434: Unrestricted Upload of File with Dangerous Type* vulnerability exists that could lead to remote code execution through a number of paths, when an attacker, writes arbitrary files to folders in context of the DC module, by sending constructed messages on the network.

CVE ID: **CVE-2021-22804**

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

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory* vulnerability exists that could cause disclosure of arbitrary files being read in the context of the user running IGSS, due to missing validation of user supplied data in network messages.

Schneider Electric Security Notification

CVE ID: **CVE-2021-22805**

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

A *CWE-306: Missing Authentication for Critical Function* vulnerability exists that could cause deletion of arbitrary files in the context of the user running IGSS due to lack of validation of network messages.

Remediation

Version 15.0.0.21244 of the IGSS DC module: dc.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:

- Only accept incoming connections from machines, which name have been added as a Station in the IGSS System Configuration module by setting the registry key called "MatchWinName" to 1 under: "HKEY_CURRENT_USER\SOFTWARE\Schneider Electric\IGSS32\V15.00.00\DC_HKLM\"
- 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 researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2021-22802, CVE-2021-22803, CVE-2021-22804, CVE-2021-22805	Vyacheslav Moskvin 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

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 *12 October 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.10.10 02:06:01 -04'00'