Schneider Electric Security Notification

IGSS (Interactive Graphical SCADA System)

10 March 2020

Overview

Schneider Electric is aware of multiple vulnerabilities in the IGSS product.

Affected Product(s)

IGSS versions 14 and prior using the service: IGSSupdate.

Vulnerability Details

CVE ID: **CVE-2020-7478**

CVSS v3.0 Base Score 7.5 | (High) | CVSS3.0/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 exists which could allow a remote unauthenticated attacker to read arbitrary files from the IGSS server PC on an unrestricted or shared network when the IGSS Update Service is enabled.

CVE ID: **CVE-2020-7479**

CVSS v3.0 Base Score 7.8 | (High) | CVSS.3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A CWE-306: Missing Authentication for Critical Function vulnerability exists which could allow a local user to execute processes that otherwise require escalation privileges when sending local network commands to the IGSS Update Service.

Remediation

These vulnerabilities are fixed in IGSS14 version 14.0.0.20009 and the update is available for download below:

http://igss.schneider-electric.com/igss/igssupdates/v140/IGSSUPDATE.zip

For IGSS version 13 and prior we recommend updating to IGSS version 14.

Alternatively, the following workarounds and mitigations can be applied by customers to reduce the risk:

- Disable the IGSS Update service when it is not required installing updates using the service.
- Keep the infrastructure offline and do not allow Windows login and network access for untrusted people and sources.

Product Information

IGSS (Interactive Graphical SCADA System) is a state-of-the art SCADA system used for monitoring and controlling industrial processes. IGSS communicates with all major industry standard PLC drivers.

Product Category - Industrial Automation Control

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

To check if your system is affected open the file Properties of IGSSupdateService.exe. The file can be located in the IGSS installation folder, typically: C:\Program Files (x86)\Schneider Electric\IGSS32\V14.0\GSS

If the Product version is lower than 14.0.0.20009 the vulnerability is present.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the "Program" mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or 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), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2020-7478, CVE-2020-7479	Trend Micro Zero Day Initiative (ZDI)

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, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.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 **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *10 March 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.03.09 21:41:48 -04'00'