Schneider Electric Security Notification

ISaGRAF Workbench for SAGE RTU

11 October 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in the third party ISaGRAF Workbench software used by SAGE RTU products.

The SAGE RTU products are hardware devices that collect utility substation information from different devices and passes it along to a SCADA software platform.

Failure to apply the mitigations provided below may risk remote code execution, which could result in privilege escalation that will allow an attacker to gain the privileges of the software. If the software is running at SYSTEM level, an attacker may gain admin level privileges. These vulnerabilities can only be exploited when users open the TCP listening ports on the RTU and connect with ISaGRAF Workbench.

Affected Products and Versions

Product	Version
SAGE RTU C3414 CPU (Current) *with optional ISaGRAF software versions prior to 6.6.10*	All firmware versions prior to C3414-500-S02K5_P5
SAGE RTU C3413, C3412 CPU (Obsolete CPUs) *with optional ISaGRAF software versions prior to 6.6.10*	All firmware versions

Note: The ISaGRAF software is an optional feature that is not part of the standard RTU Firmware package, so if this option is not purchased, the vulnerabilities mentioned in this notification are not applicable.

Vulnerability Details

CVE ID: **CVE-2022-2463**

CVSS v3.1 Base Score 6.1 | Medium | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

ISaGRAF Workbench software versions 6.0 through 6.6.9 are affected by a Path Traversal vulnerability. A crafted malicious .7z exchange file may allow an attacker to gain the privileges of the ISaGRAF Workbench software when opened. If the software is running at the SYSTEM level, then the attacker will gain admin level privileges. User interaction is required for this exploit to be successful.
Note: The CVSS score provided above is calculated in the context of SAGE RTU.

CVE ID: **CVE-2022-2464**

CVSS v3.1 Base Score 6.1 | Medium | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

ISaGRAF Workbench software versions 6.0 through 6.6.9 are affected by a Path Traversal vulnerability. Crafted malicious files can allow an attacker to traverse the file system when opened by ISaGRAF Workbench. If successfully exploited, an attacker could overwrite existing files and create additional files with the same permissions of the ISaGRAF Workbench software. User interaction is required for this exploit to be successful.
Note: The CVSS score provided above is calculated in the context of SAGE RTU.

CVE ID: **CVE-2022-2465**

CVSS v3.1 Base Score 6.1 | Medium | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

ISaGRAF Workbench software versions 6.0 through 6.6.9 are affected by a Deserialization of Untrusted Data vulnerability. ISaGRAF Workbench does not limit the objects that can be deserialized. This vulnerability allows attackers to craft a malicious serialized object that, if opened by a local user in ISaGRAF Workbench, may result in remote code execution. This vulnerability requires user interaction to be successfully exploited.
Note: The CVSS score provided above is calculated in the context of SAGE RTU.

Mitigation

Affected Product & Version	Mitigation
SAGE RTU C3414 CPU (Current) with optional ISaGRAF software *All firmware versions prior to C3414-500-S02K5_P5*	Version C3414-500-S02K5_P5 of SAGE RTU CPU 3414 includes a mitigation for these vulnerabilities and is available for download here: https://www.sage-rtu.com/downloads.html Reboot of SAGE RTU is required after firmware upgrade. This mitigation disables the ISaGRAF listening TCP ports by default and provides an additional network service checkbox to allow customers to enable the ISaGRAF ETCP task, which will open the TCP listening ports to connect with ISaGRAF workbench when needed, and to disable the TCP listening ports when ISaGRAF Workbench development, debugging, and downloading tasks are complete. These vulnerabilities can only be exploited when users reopen the listening ports and connect with ISaGRAF workbench. These vulnerabilities only apply when a non-secure network is being used to perform development tasks in non-runtime applications. It is our recommendation to mitigate these vulnerabilities by performing all ISaGRAF workbench tasks on a secure network or on a private network when connecting to the device. OR

	If firmware is not upgraded to C3414-500-S02K5_P5, but customers are running firmware version C3414-500-S02K2 or above, then they should immediately apply the following mitigations to reduce the risk of exploit: If ISaGRAF is configured and in use, the built-in firewall can be used to disable ISaGRAF port 1131 and 1113 when the debugger is not in use. Use the following commands in the Firewall configuration to disable external access to ISaGRAF: Block in proto tcp from any to any port = 1131 Block in proto tcp from any to any port = 1113 If ISaGRAF is NOT configured and in use, the ISaGRAF port is by default not enabled and does not start automatically, therefore there is no impact of these vulnerabilities, and no further action is required by customers.
SAGE RTU C3413, C3412 CPU (Obsolete CPUs) with optional ISaGRAF software *All firmware versions*	SAGE RTU CPU's C3413 and C3412 have reached their end of life and are no longer supported. Customers should immediately upgrade to the latest CPU C3414 and apply C3414-500-S02K5_P5 or later firmware which can be downloaded here: https://www.sage-rtu.com/downloads.html Reboot of SAGE RTU is required after firmware upgrade. This mitigation disables the ISaGRAF listening TCP ports by default and provides an additional network service checkbox to allow customers to enable the ISaGRAF ETCP task, which will open the TCP listening ports to connect with ISaGRAF workbench when needed, and to disable the TCP listening ports when ISaGRAF Workbench development, debugging, and downloading tasks are complete. These vulnerabilities can only be exploited when users reopen the listening ports and connect with ISaGRAF workbench. These vulnerabilities only apply when a non-secure network is being used to perform development tasks in non-runtime applications. It is our recommendation to mitigate these vulnerabilies by performing all ISaGRAF workbench tasks on a secure network or on a private network when connecting to the device.

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.

Schneider Electric Security Notification

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.

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

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

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 *11 October 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.10.10 13:20:48 -04'00'