Schneider Electric Security Notification

ISaGRAF Vulnerabilities

in IEC 61131-3 Programming and Engineering Tools

08 June 2021 (12 March 2024)

Overview

On June 8, 2021, Rockwell Automation disclosed multiple vulnerabilities in its ISaGRAF Workbench and ISaGRAF Runtime products. Multiple vendors, including Schneider Electric, embed ISaGRAF in their offers.

ISaGRAF Workbench is used to program applications for embedded devices using IEC 61131-3 languages and may be incorporated into larger programming and configuration tools. The ISaGRAF Runtime module executes the process control code created in ISaGRAF Workbench on embedded devices.

If successfully exploited, bad actors could execute a range of actions, including accessing and disclosing sensitive information, privilege escalation, and in some cases remote code execution.

Customers should immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves from possible exploitation of these vulnerabilities. Where appropriate, this includes locating their industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission-critical systems and devices from being accessed from outside networks; and following the mitigations and general security recommendations below.

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's Customer Care Center.

Subscribe to the Schneider Electric security notification service to be informed of critical updates to this notification, including information on affected products and remediation plans: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

March 2024 Update: New mitigations for Saitel DP and Saitel DR are available for download (page 5).

Vulnerability Details

Additional details on these specific vulnerabilities can be found in the Rockwell Automation disclosure (requires a login) and the ICS-CERT advisory.

- CVE-2020-25176
- CVE-2020-25178
- CVE-2020-25182
- CVE-2020-25184
- CVE-2020-25180

Schneider Electric Security Notification

Affected Products & Remediations

Affected Product and Versions	Remediation
SAGE RTU - C3414 CPU *All versions prior to C3414-500-S02K5_P5*	Version C3414-500-S02K5_P5 of SAGE RTU CPU 3414 includes a fix for this vulnerability and is available for download here: https://www.sage-rtu.com/downloads.html Reboot of SAGE RTU is required after firmware upgrade. This fix disables ISaGRAF by default and provides an additional network service checkbox to allow you to enable the ISaGRAF ETCP task, which will open listening ports to connect with ISaGRAF workbench when needed. OR If the firmware is not upgraded to C3414-500-S02K5_P5, but you are at firmware version C3414-500-S02K2 or above customers 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 issue or required actions.
SAGE RTU - C3413 CPU **C3412 CPU** *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 fix disables ISaGRAF by default and provides an additional network service checkbox to allow you to enable the ISaGRAF ETCP task, which will open listening ports to connect with ISaGRAF workbench when needed.

SCADAPack 300E RTU **SCADAPack 53xE RTU** *SCADAPack E firmware 8.18.1 and prior*	Version 8.19.1 of SCADAPack Workbench includes a fix for these vulnerabilities and is available for download here: https://shop.exchange.se.com/en-US/apps/62865/scadapack-e-workbench-and-utilities. A reboot is required when upgrading to new firmware. No user actions are required to apply the remediation beyond upgrading the firmware in the RTU. To verify the remediation is in place, use SCADAPack E Configurator or the RTU command line to display the firmware version.
SCADAPack Workbench *SCADAPack Workbench 6.6.8 and prior*	
SCD2200 Firmware for CP-3/MC-31 *SCD2200 Firmware 10024 and prior*	Customers should upgrade to the firmware V9.1.0 or later (14942), which incorporates ISaGRAF Workbench V6.6.9. Notification of firmware release can be found here: https://secommunities.force.com/PAkb/s/article/CCN000244525 A reboot is required when upgrading to new firmware. No user actions are required to apply the remediation beyond upgrading the firmware in the RTU.

Affected Products

Schneider Electric continues to assess how these vulnerabilities affect its offers and is establishing a remediation plan for the affected offers listed below. The company will continue to update this notification as additional offer-specific information becomes available.

Until then, customers should immediately:

- Implement firewall rules to restrict or block access on TCP port 1131 from outside the industrial control system.
- Disable the ISaGRAF/TCP service when not required. Typically, this service is needed only during commissioning or maintenance operations.
- Limit and control administrative access rights for ISaGRAF services.

For additional product specific advice see the table below.

Mitigations

Affected Product and Version	Mitigations
PowerLogic T300 (formerly Easergy T300) *T300 v2.8.2 and prior*	New mitigations for the PowerLogic T300 are available for download. These mitigations reduce, but do not eliminate the risk of this vulnerability. Firmware v2.9.0 (or later) for the T300 is available for download here: https://www.se.com/ww/en/download/document/T300_Firmware/ If you cannot update to v2.9.0 (or later) please note the following. Customers should use the product firewall to block the TCP port 1131 and only unblock it during new program upgrade/debug. If ISaGRAF is not configured, the service is not active and the port is closed, then no further action is required.
Easergy C5 *Versions up to 1.0.x and embedding ISaGRAF v5.2 and prior* **MiCOM C264** *Versions up to D6.x with embedded ISaGRAF v5.2 and prior*	ISaGRAF program upload/debug mode is disabled by default, after enabling for product commissioning, disable ISaGRAF program upload/debug mode. **NOTE:** New mitigations are available for this product. These mitigations reduce, but do not eliminate the risk of this vulnerability. Please contact your authorized service provider / customer care and request MiCOM C264 D7.21 (or later) OR Easergy C5 1.1.6 (or later).
PACiS GTW **EPAS GTW** *All gateway versions supporting ISaGRAF 5.2 and prior:* *Windows:* – *PACiS GTW 5.1* – *PACiS GTW 5.2* – *PACiS GTW 6.1* – *PACiS GTW 6.3* – *EPAS GTW 6.4* *Linux:* – *PACiS GTW 6.3* – *EPAS GTW 6.4*	If ISaGRAF is configured, customers should use the OS firewall to block TCP port 1131 and only unblock it during new program upgrade/debug. For detailed instructions, please contact your Schneider Electric representative and request “GTW ISaGRAF vulnerabilities mitigation plan.” **NOTE:** New mitigations are available for this product. These mitigations reduce, but do not eliminate the risk of this vulnerability. Please contact your authorized service provider / customer care and request EPAS Gateway v6.4.615.100.102 or later.

Saitel DP *v11.06.21 and prior*	New mitigations for Saitel DP are available for download. These mitigations reduce, but do not eliminate the risk of this vulnerability. Firmware SM_CPU866e v11.06.32 (or later) for Saitel DP is available for download here: https://www.se.com/ww/en/product-range/61747-saitel-dp/#software-and-firmware If you cannot update to Firmware SM_CPU866e v11.06.32 (or later) please note the following. Customers should use the product firewall to block the TCP port 1131 and only unblock it during new program upgrade/debug. If ISaGRAF is not configured, the service is not active and the port is closed, then no further action is required.
Saitel DR *v11.06.12 and prior*	New mitigations for Saitel DR are available for download. These mitigations reduce, but do not eliminate the risk of this vulnerability. Firmware HUe v11.06.27 (or later) for Saitel DR is available for download here: https://www.se.com/ww/en/product-range/62685-saitel-dr-remote-terminal-unit-controller#software-and-firmware If you cannot update to Firmware HUe v11.06.27 (or later) please note the following. Customers should use the product firewall to block the TCP port 1131 and only unblock it during new program upgrade/debug. If ISaGRAF is not configured, the service is not active and the port is closed, then no further action is required.
SCD2200 Firmware for CP-3/MC-31 *SCD2200 Firmware 10024 and prior*	Implement firewall rules to restrict or block access on TCP port 1131 from outside the industrial control system. Disable the ISaGRAF/TCP service when not required. Typically, this service is needed only during commissioning or maintenance operations. Limit and control administrative access rights for ISaGRAF services.

Talus T4e RTU **Talus T4c RTU** *T4e Mk 1:* *A18.xx Firmware (all)* *T4e Mk II & T4c:* *A19.08 Firmware and prior*	Implement firewall rules to restrict or block access on TCP port 1131 from outside the industrial control system. Disable the ISaGRAF/TCP service when not required. Typically, this service is needed only during commissioning or maintenance operations. Limit and control administrative access rights for ISaGRAF services. Upgrade to ISaGRAF 6.6.9 (A19.09 Firmware or later).

For more details and assistance on how to protect your installation, please contact your local Schneider Electric Industrial Cybersecurity Services organization, which is fully aware of this situation and can support you through the process.

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.
- 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 security controls.
- 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 best practices refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

For More Information

Schneider Electric Security Notification

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

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 1.0.0 *08 June 2021*	Original Release
Version 2.0.0 *14 September 2021*	Added remediations for SAGE RTU C3414 CPU, C3413 CPU and C3412 CPU (page 2)

Schneider Electric Security Notification

Version 3.0.0 *09 November 2021*	Added remediations for SCADAPack 300E RTU, SCADAPack 53xE RTU, and SCADAPack Workbench (page 2)
Version 4.0.0 *08 November 2022*	Talus T4e and T4c RTUs were added as affected products along with a mitigation (page 5).
Version 5.0.0 *14 March 2023*	A remediation is available for SCD2200 product (page 3).
Version 6.0.0 *09 January 2024*	New mitigations for PowerLogic T300, MiCOM C264 D7.21 (or later) OR Easergy C5 1.1.6 (or later), PACiS GTW, and EPAS GTW are available for download (page 4).
Version 7.0.0 *12 March 2024*	New mitigations for Saitel DP and Saitel DR are available for download (page 5).

Product Security Office

Digitally signed by Product Security Office
Date: 2024.03.11 14:41:59 -04'00'