OVARRO
CONNECTING TECHNOLOGIES

Security Advisory ISaGRAF Workbench

SEP-SA-2022-0001

Revision History

Version	Date	Description
1	30/08/2022	Initial Release

Executive Summary

- **Document Type**: Security Advisory (Seprol RTUs)
- **Reference**: SEP-SA-2022-0001
- **Vulnerabilities**: CVE-2022-1018, CVE-2022-2463, CVE-2022-2464 & CVE-2022-2465 disclosed by Rockwell Automation for ISaGRAF Workbench
- **Publisher**: Ovarro
- **Contact**: cybersecurity@ovarro.com
- **Current Status**: Preliminary
- **Current Version**: 1.0
- **Initial Release Date**: 30/08/2022
- **Latest Release Date**: 30/08/2022

Risk Evaluation

As the Seprol range of S2000 WITS RTUs uses the ISaGRAF Workbench, the risks are the same as the ones disclosed by Rockwell Automation.

Successful exploitation of these vulnerabilities could allow an attacker to pass local file data to a remote web server, leading to loss of confidentiality and could result in directory traversal, privilege escalation, and arbitrary code execution.

Technical Details

Affected Products

ISaGRAF Workbench V6 up to and including V6.6.9

Vulnerability Overview

CVE-2022-1018, CVE-2022-2463, CVE-2022-2464 & CVE-2022-2465 disclosed by Rockwell Automation for ISaGRAF Workbench are described in the following links.

Sources

Rockwell Automation ISaGRAF (Update A) | CISA

Rockwell Automation ISaGRAF Workbench | CISA

Mitigations

ISaGRAF Workbench V6.6.10 is now available to download either directly from the Rockwell download centre https://compatibility.rockwellautomation.com/Pages/home.aspx or from the Ovarro FTP server ftps://ftp.ovarro.com.

As stated by Rockwell Automation, the following mitigations should be applied:

- Run Connected Components Workbench as a User, not as an Administrator, to minimize the impact of malicious code on the infected system.
- Do not open untrusted files, and more specifically untrusted .7z exchange files with, ISaGRAF Workbench. Employ training and awareness programs to educate users on the warning signs of a phishing or social engineering attack.
- Use Microsoft AppLocker or other similar allow list application to help mitigate risk.
- Ensure the least-privilege user principle is followed, and user/service account access to shared resources (such as a database) is only granted with a minimum number of rights as needed.

In addition to the above, the following S2000 specific mitigation measures could also be applied until WB V6.6.10 can be deployed

- Use CA Tools V6.14 or above to disable the any ISaGRAF workbench from downloading files to an RTU once the RTU is commissioned. Select the **Isagraf ETCP** option in the **IP Security** tab within the BCF using CA Tools

OVARRO
CONNECTING TECHNOLOGIES