OVARRO
CONNECTING TECHNOLOGIES

Security Advisory

KF-SA-2022-0001

Revision History

Version	Date	Description
1	29/08/2022	Initial Release

Executive Summary

- **Document Type**: Security Advisory
- **Reference**: KF-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**: 29/08/2022
- **Latest Release Date**: 29/08/2022

Risk Evaluation and overview

Kingfisher Toolbox Plus software uses Rockwell Automation's ISaGRAF Workbench as an integrated configuration and programming solution.

Rockwell Automation has posted the above listed vulnerabilities for ISaGRAF Workbench.

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.

Due to the way Toolbox PLUS integrates ISaGRAF Workbench, customers projects are not directly exposed to these vulnerabilities.
Example. The standard .7z exchange files do not work within ToolboxPLUS projects because of the way we have defined our default projects.)

However, ISaGRAF Workbench is installed on the users' computer as a standalone piece software and can be opened and used individually for any other purpose. The Workbench itself (prior to v6.6.10) can be manipulated and put users at risk.

So, while Kingfisher systems are not affected, users might be.

Technical Details

Affected Products

Kingfisher Toolbox Plus up to version 9.0

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

Ovarro is working on a new release of Kingfisher Toolbox Plus (version 9.1) that will include ISaGRAF Worbench 6.6.10 with all the fixes for these vulnerabilities.

Pending the new release, the following mitigations should be applied:

- For Kingfisher systems, Ovarro recommend users create projects using ToolboxPLUS only and discourage the direct use of ISaGRAF. Using ISaGRAF directly may exploit the known/unknown vulnerabilities in ISaGRAF.
- For Open ISaGRAF systems, Rockwell Automation advise the following.
  - 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.

OVARRO

CONNECTING TECHNOLOGIES