DOCUMENT ID: 9AKK108469A2889
REVISION: A
DATE: 2024-03-27

CYBER SECURITY NOTIFICATION

ABB ISaGRAF Workbench (2104764)

Multiple Vulnerabilities in ISaGRAF Workbench v6.6.0

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, expressed or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Purpose

ABB has a rigorous cyber security program which involves not only internal processes to ensure product security, but also external engagement with the wider cybersecurity community and 3rd party suppliers. Occasionally, an issue is identified with the potential to impact ABB products and systems.

Generally, this means 3rd party product vulnerabilities or life-cycle issues to which ABB products may have a dependency on. Another example could be threats which are not directly targeting ABB products, however may constitute a threat to environments where ABB products/systems operate.

When a potential threat is identified or reported, ABB immediately initiates our vulnerability handling process. This entails an evaluation to determine if there are steps which can be taken to reduce risk and maintain functionality for the end user.

The result may be the publication of a Cyber Security Notification. This intends to notify customers of the issue and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible.

The release of a Cyber Security Notification should not be assumed as an indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Notification is an example of ABB's commitment to the user community in support of this critical topic. The release of a Notification intends to provide timely information which is essential to help ensure our customers are fully informed. See details below and refer to the section on "General security recommendations" for further advise on how to keep your systems secure.

Background

ABB is aware of public reports of vulnerabilities in the Rockwell Automation® ISaGRAF® Workbench v6.6.0. ABB redistributes this software as ABB ISaGRAF Workbench (2104764).

The vulnerabilities require user interaction to be exploited. If successfully exploited, these vulnerabilities may result in information leakage and loss of confidentiality, directory traversal, privilege escalation, and arbitrary code execution.

See the links to the Rockwell advisories listed in later sections for full information.

Vulnerability Details

CVE-2022-2465: Deserialization of untrusted data may result in arbitrary code execution

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.

– CVSS v3.1 Base Score: 8.6/10[HIGH]

– CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVE-2022-2464: Directory traversal vulnerability may lead to privilege escalation

The parsing mechanism that processes certain file types does not provide input sanitization for file paths. This may allow an attacker to craft malicious files that, when opened by ISaGRAF Workbench, can traverse the file system. If successfully exploited, an attacker would be able to 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.

- CVSS v3.1 Base Score: 7.7/10[HIGH]
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

CVE-2022-2463: Improper input sanitization may lead to privilege escalation

ISaGRAF does not sanitize paths specified within the .7z exchange file during extraction. This type of vulnerability is also commonly referred to as a Zip Slip. A local, authenticated attacker can create a malicious .7z exchange file that when opened by ISaGRAF Workbench will allow the attacker to gain the privileges of the software. If the software is running at SYSTEM level, the attacker will gain admin level privileges. User interaction is required for this exploit to be successful.

- CVSS v3.1 Base Score: 6.1/10[MEDIUM]
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

CVE-2022-1018 XML External Entity Leads to Information Leak

When opening a malicious solution file provided by an attacker, the application suffers from an XML External Entity vulnerability due to an unsafe call within a dynamic link library file.

As a result, this could be exploited to pass data of local files of the victim to a remote web server controlled by an attacker leading to a loss of confidentiality.

- CVSS v3.1 Base Score: 5.5/10 [Medium]
- CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Affected product

After investigating all ABB related products, it is determined that only the ISaGRAF Workbench v6.6.0 software (2104764) that is distributed by ABB is affected.

Recommended immediate actions

Follow the mitigations recommended in the Rockwell Automation security advisories (login required):

- File Parsing XML Entity in Multiple Products
- ISaGRAF Workbench Vulnerable to Multiple Phishing-Style Attacks

ABB recommends:

- Do not run ISaGRAF Workbench with Administrator privileges.

- Employ least-privilege user principles.
- Do not open untrusted files with ISAGRAF Workbench.

General security recommendations

For any installation of software-related ABB products, we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system and firmware patches as well as anti-virus and firewall.
- 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.

Support

For additional instructions and support, please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2024-03-27