The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

07/29/2021

SUBJECT:

Multiple Vulnerabilities in Rockwell Automation ISaGRAF5 Runtime Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Rockwell Automation ISaGRAF5 Runtime, the most severe of which could allow for remote code execution. These affected Industrial Control System (ICS) products are used across several sectors, including chemical, critical manufacturing, food and agriculture, water and wastewater systems and others. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to perform remote code execution on the affected device.

THREAT INTELLIGENCE:

There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- AADvance Controller version 1.40 and earlier
- ISaGRAF Free Runtime in ISaGRAF6 Workbench Version 6.6.8 and earlier
- Micro800 family, all versions
- GE Steam Power's ALSPA S6 MFC3000 and MFC1000 (all versions)
- Xylem MultiSmart Gen-1 devices and MultiSmart Gen-2 devices running firmware prior to Version 3.2.0 (**If ISaGRAF is enabled on those devices**)

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Rockwell Automation ISaGRAF5 Runtime which could allow for remote code execution. Details of these vulnerabilities are as follows:

- Some commands used by the ISaGRAF eXchange Layer (IXL) protocol perform various file operations in the file system. Since the parameter pointing to the file name is not checked for reserved characters, it is possible for a remote, unauthenticated attacker to traverse an application's directory, which could lead to remote code execution. (CVE-2020-25176)
- ISaGRAF Runtime stores the password in plaintext in a file that is in the same directory as the executable file. ISaGRAF Runtime reads the file and saves the data in a variable without any additional modification. A local, unauthenticated attacker could compromise the user passwords, resulting in information disclosure. (CVE-2020-25184)
- ISaGRAF Workbench communicates with ISaGRAF Runtime using TCP/IP. This communication protocol provides various file system operations, as well as the uploading of applications. Data is transferred over this protocol unencrypted, which could allow a remote unauthenticated attacker to upload, read, and delete files. (CVE-2020-25178)
- ISaGRAF Runtime searches for and loads DLLs as dynamic libraries. Uncontrolled loading of dynamic libraries could allow a local, unauthenticated attacker to execute arbitrary code. This vulnerability only affects ISaGRAF Runtime when running on Microsoft Windows systems. (CVE-2020-25182)
- ISaGRAF Runtime includes the functionality of setting a password that is required to execute privileged commands. The password value passed to ISaGRAF Runtime is the result of encryption performed with a fixed key value using the Tiny Encryption Algorithm (TEA) on an entered or saved password. A remote, unauthenticated attacker could pass their own encrypted password to the ISaGRAF 5 Runtime, which may result in information disclosure on the device. (CVE-2020-25180)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Rockwell Automation to vulnerable systems immediately after appropriate testing.
- Isolate control systems from other networks when possible.
- Minimize network exposure for all control system devices.
- Remind users not to download, accept or execute files from untrusted and unknown sources.
- Remind users not to visit untrusted websites or follow links provided by untrusted or unknown sources.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
ICS-CERT:
https://us-cert.cisa.gov/ics/advisories/icsa-20-280-01

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25176
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25178
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25180
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25182
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25184