GE
Steam Power
Automation & Controls

October 19, 2022	CYBERSECURITY	ALSPA S6 MFC3000, MFC1000

Topic: Vulnerability "CVE-2020-25182, CVE-2020-25176, CVE-2020-25178, CVE-2020-25184, CVE-2020-25180 "in MFC3000 and MFC1000 controller all versions

Dear Valued Customer,

Summary:

A vulnerability report has been reported from Kaspersky about vulnerability in ISaGRAF® Runtime 4 and 5 software provide by Rockwell Automation.
ISaGRAF® is a component of our MFC3000 and MFC1000 controllers. If successfully exploited, these vulnerabilities may result in remote code execution, information disclosure, or denial of service.

Via the ICS Advisory -advisory referenced vulnerability's "ICSA-20-280-01".

A successful exploitation of this vulnerability could lead to information disclosure on the device and allow an unauthenticated attacker to execute arbitrary code.

Details of this vulnerability are available on the ICS security advisory web site:
on the site ICSA-20-280-01
and on the Rockwell Automation site: Industrial Security Advisory
The product affected are:

- ALSPA S6 MFC3000 all versions
- ALSPA S6 MFC1000 all versions

Vulnerability detail:

UNCONTROLLED SEARCH PATH ELEMENT Path Element CWE-427

The product uses a fixed or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors.

CVE-2020-25182 has been assigned to this vulnerability. A CVSS v3.1 base score of 6.7 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).

RELATIVE PATH TRAVERSAL CWE-23

The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.

CVE-2020-25176 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.1 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).

to CLEARTEXT TRANSMISSION OF SENSITIVE INFORMATION, CWE-319

The software transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

CVE-2020-25178 has been assigned to this vulnerability. A CVSS v3.1 base score of 7.5 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).

USE OF HARD CODED CRYPTOGRAPHIC KEY, CWE-321

The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered.

CVE-2020-25180 has been assigned to this vulnerability. A CVSS v3.1 base score of 6.5 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).

UNPROTECTED STORAGE OF CREDENTIALS CWE-256

Storing a password in plaintext may result in a system compromise.

CVE-2020-25184 has been assigned to this vulnerability. A CVSS v3.1 base score of 7.8 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).

Defense in depth

To minimize the risk of exposure to vulnerability's, GE recommends implementing defense in depth strategy for critical process control system.

Specifically, for this point GE recommends users take these defensive measures to minimize the risk of exploitation of this vulnerability:

- Minimize network exposure for all control system devices and/or systems and ensure that they are not accessible from the internet without adequate protection (UTM, DMZ, IDS, ...).
- Locate control system networks (Alspa networks: Ethernet Entreprise Network, Ethernet Process Network S8000, Field Network F8000 or EPL) and third party connected equipment (through Modbus, Profibus, IEC104, ...) behind firewalls and isolate them from the business or other network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.
- Restrict system access to authorized personnel only and follow a least privilege approach (access control, locked room, video, ...).

GE reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

GE
Steam Power
Power Automation & Controls

GE Power Automation & Control Contact information

To mitigate this subject GE has developed a dedicated hardened firmware process that we can apply to all of our customer controller MFC3000 V1+ release and higher. The main target of this firmware is to reduce the risk of exploitation exposure, at an acceptable level from GE perspective, at the controller level.

We will be please to support the enhancement of the cyber security of your equipment with improved solution product update or dedicated MFC controller hardening. We can conduct a thorough analysis of your cyber security need stop define the optimal solution. If you would like to assess the level of your cybersecurity level, please contact us

Contact your GE Steam Power account manager or our Help Desk at +33 1 60 13 43 91 / helpdesk.control-systems@ge.com for help on ordering or cybersecurity services.

Hugues Moreau
Product Manager Power Automation & Controls, GE Steam Power
Hugues.moreau@ge.com

Revision History

Version	Release Date	Purpose
A	june 17, 2021	Initial version
B	june 20, 2022	Add capacity to do dedicated MFC controller hardening for this vulnerability and MFC3000 V1+ release and higher.
C	October 19, 2022	Add GE mitigation – MFC3000 V1° hardening