GE
Steam Power
Automation & Controls

July 22nd, 2021	CYBERSECURITY	OPC Tunneller and Gateway

Topic: Vulnerability "CVE-2020-27297, CVE-2020-27299, CVE-2020-27274, CVE-2020-27295, CVE-2020-14524, CVE-2020-14522 "in Alspa OPC tunneller and Gateway

Dear Valued Customer,

The purpose of this Service Bulletin is to inform you about a potential cyber vulnerability that may affect your Alspa system.

The vulnerability described below may have some impact on your Matrikon OPC tunneller or Softing Industrial Automation OPC prior to version 4.47.0 .

Via the ICS Advisory referenced vulnerability's "ICSA-21-021-03"and "ICSA-20-210-02", a hacker could take advantage of these vulnerabilities, to get sensitive information, remotely execute arbitrary code, or crash the device.

Details of these vulnerabilities are available on the ICS security advisory web site:
on the site https://us-cert.cisa.gov/ics/advisories/icsa-21-021-03
and https://us-cert.cisa.gov/ics/advisories/icsa-21-210-02

The products affected for Matrikon are:

- Alspa gateway type CSSF T3000, OPC,

connection between HMI and third party using matrikon OPC tunnellerThe products affected for softing is:

- Alspa gateway type AC800

We have identified that your system may be affected by these vulnerabilities. To treat these vulnerabilities GE strongly recommend to:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the internet
- Locate control system networks and remote devices behind firewalls and isolate them from the business 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.

We also strongly recommend performing impact analysis and risk assessment prior to deploying defensive measures.

Defense in depth

The above proposed recommendations are part of a defense in-depth strategy. Other solutions / tools may be available to strengthen this defense in depth strategy. To minimize the risk of exposure to the identified vulnerabilities and others to come, GE recommend implementing a comprehensive defense in depth strategy for critical process control system.

GE Power Automation & Control Contact information

We will be please to support the enhancement of the cyber security of your equipment with improved solution, or product update. 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 Power Automation & Controls sales person 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