GE
Steam Power
Power Automation & Controls

June 22, 2023 **CYBERSECURITY**

Topic: "COSMICENERGY : New OT Malware Possibly Related To Russian Emergency Response Exercises."

GE Steam Power is aware of a "*COSMICENERGY : New OT Malware*

Mandiant identified novel operational technology (OT) / industrial control system (ICS)-oriented malware, which we track as COSMICENERGY, uploaded to a public malware scanning utility in December 2021 by a submitter in Russia. The malware is designed to cause electric power disruption by interacting with **IEC 60870-5-104 (IEC-104)** devices, such as remote terminal units (RTUs), that are commonly leveraged in electric transmission and distribution operations in Europe, the Middle East, and Asia.

Impacted products are all products with IEC 104 Server function, identified as potential target for this malware as :

- ALSPA Series 6 CSS-G IEC104,
- ALSPA Series 5 CSS-G IEC104,
- ALSPA MFC3000 controller with IEC104 communication

To treat this vulnerability GE recommends to check that there is relevant defense in depth security measures in place.

It is also recommended to check if there is any trace of this malware introduction in the system. The necessary treat intelligence to detect it is described in the following link cosmicenergy-ot-malware-russian-response – Discovery method

Defense-in-depth

To minimize the risk of the exploitation of current and future system vulnerabilities, GE Steam Power highly recommends implementation of a defense-in-depth strategy (complementary defenses in Physical, Technical, and administrative domains) for your critical process control systems.

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 outside of the DCS.
- When external communication 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.

- Follow good network design practices, such as implementing network segmentation, and use DMZs with properly configured firewalls to selectively control, and monitor all traffic passed between zones and systems.
- Monitor and log all network traffic attempting to reach affected products for suspicious activity.
- Close all unused ports on affected systems.
- Restrict system access to authorized personnel only and follow a least privilege approach.
- Perform access control checks to limit which users can access the feature that requires the hard-coded credentials. For example, a feature might only be enabled through the system console instead of through a network connection.

We will be pleased to support you in the enhancement of your cybersecurity strategy and improve or update your current equipment with latest cybersecurity methodologies and solutions. We suggest that a thorough analysis of your cybersecurity status be performed and resulting recommendations for an optimal solution be implemented according to the level of risk exposure and/or the standard frameworks which are applicable to your needs.

Contact your GE Power Automation & Controls salesperson or our Help Desk at +33 1 60 13 43 91 / helpdesk.control-systems@ge.com for help with ordering cybersecurity services and solutions.

Thierry PELET
Product Security Leader, GE Steam Power
thierry.pelet@ge.com

Revision History

Version	Release Date	Purpose
A	June 22, 2023	Initial version