GE
Steam Power
Power Automation & Controls

February 01, 2022 **CYBERSECURITY**

Topic: Apache Log4j Vulnerability CVE-2021-44228, CVE-2021-4104, CVE-2021-45046, CVE-2021-45105.

Dear Valued Customer,

Summary:

GE Steam Power is aware of security vulnerabilities identified in CVE-2021-44228, CVE-2021-4104, CVE-2021-45046, CVE-2021-45105. These vulnerabilities are being referred to as Log4jShell and are reported to be under active exploitation. Immediately upon learning of these vulnerabilities, GE Steam Power initiated its cyber response plans to identify and mitigate potential risks both within its own environment and within its products. GE Steam Power has also deployed specific Log4j threat protections and detections across our host, email, network, and cloud attack surfaces.

Further to our updated analyses, the following GE Steam Power products are **not** impacted by these vulnerabilities:

- ALSPA Series 6 HMI software version 6.3 and older
- ALSPA Series 6 Controcad software version 5.3 and older
- ALSPA Series 6 MFC Controller,
- Generator Health Monitoring software,
- Alspa PAM Large Size Plant software,
- Alspa PAM Small Size Plant software,
- ALSPA P320 Series 5 Centralog HMI & Controcad software,
- ALSPA P320 Series 3&4 Centralog HMI software, (CCC, HDSR, CVS, CIS)
- ALSPA P320 Series 3&4 Engineering software, (P4, Microete, Controcad Unix)
- Mark Vie Control ST software.

The following GE Steam Power products are impacted by these vulnerabilities:

Product	**Source of analysis**	**Remediation**
Mark Vie Control Server	*GE Gas Power Product Security* Security Bulletins and Advisories | GE Gas Power	Contact the helpdesk (helpdesk.control-systems@ge.com)for the detailed remediation procedure

GE Log Collector V2.00 and older	GE Steam Power with Graylog communication	Contact the helpdesk (helpdesk.control-systems@ge.com)for the detailed mitigation procedure.
ALSPA Series 6 HMI software version 6.4, from Oracle third party.	GE Steam Power scanning with January 2022 updated detection tool	Contact the helpdesk (helpdesk.control-systems@ge.com)for the detailed remediation procedure
ALSPA Series 6 Controcad software version 5.4, from Oracle third party.	GE Steam Power scanning with January 2022 updated detection tool	Contact the helpdesk (helpdesk.control-systems@ge.com)for the detailed remediation procedure

For third party equipment present in our standard architecture, we have requested our suppliers to deliver to us the status with respect to these vulnerabilities. We have not found affected third party software except as listed above.

Due to ongoing product enhancements, GE Steam Power reserves the right to change or update its advisories without advance notification.

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 Steam Power recommends users take these defensive measures to minimize the risk of exploitation of these vulnerabilities:

- 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 network security controls and isolate them from the business or other network.

We will continue to monitor this situation and provide updates as appropriate.
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.

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

Revision History

Version	Release Date	Purpose
A	December 14, 2021	Initial version
B	December 22, 2021	updated lists of identified impacted and non-impacted products at this date. updated list of CVE.
C	January 24, 2022	Update following vulnerability scan with updated tool integrating log4j vulnerability signature. Updated lists of identified impacted and non-impacted products at this date.
D	February 01, 2022	Update list of impacted and not impacted products with contact for remediation procedure