February 017, 2023 **CYBERSECURITY**

Topic: “CVE-2022-37958” [NVD - CVE-2022-37958 (nist.gov)]

Dear Valued Customer,

GE Steam Power is aware of a “Critical Remote Code execution Vulnerability identified in CVE-2022-3759, impacting Client-server Extended Negotiation security Mechanism, named *SPNEGO*

In September 2022, Microsoft patched an information disclosure vulnerability in SPNEGO NEGOEX (CVE-2022-37958). On December 13, Microsoft reclassified the vulnerability as “Critical” severity after IBM Security X-Force Red Security Researcher Valentina Palmiotti discovered the vulnerability could allow attackers to remotely execute code.

This vulnerability could allow an attacker to remotely execute arbitrary code by accessing the NEGOEX protocol via any Windows application protocol that authenticates, such as SMB or RDP, by default. This list of affected protocols is not complete and may exist wherever SPNEGO is in use, including in SMTP and HTTP when SPNEGO authentication negotiation is enabled, such as for use with Kerberos or Net-NTLM authentication.

Our product affected are all product based on Microsoft windows OS as :

- ALSPA Series 6 HMI software,
- ALSPA Series 6 CAC, CIS, Historian and IMS, software,
- ALSPA Series 6 Controcad software,
- ALSPA Series 6 MFC Controller,
- ALSPA P320 Series 5 Centralog HMI & Controcad softwares,
- Mark Vie Control ST software
- Patch Management Station
- Jump Station - Security Remote connection
- Alspa Anti-Malware Antivirus Si
- Back Up & Restore

Product	**Status**
ALSPA Series 6 HMI software ALSPA Series 6 CAC, CIS, Historian and IMS, software, ALSPA Series 6 Controcad software **Alspa Version Series 6.1 R5**	**Product based on Microsoft Windows 10 Operating System** If the product is updated with our patch management solution from a package dated November 2022 or later, the Microsoft corrective have already been applied. For product not updated through Patch Management contract, we recommend subscribing to our one-time patch management solution.

ALSPA Series 6 HMI software ALSPA Series 6 CAC, CIS, Historian and IMS, software, ALSPA Series 6 Controcad software **Alspa Version Series 6.1 R1-R2-R3-R4**	**Product based on Microsoft Windows 7 Operating System** Microsoft Windows 7 patch not available for Alspa Our recommendation is first to apply defense in depth strategy to reduce the risk, including disconnect the system to all ethernet external network communication and then to implement HMI Upgrade solution to Windows 10 solution.
ALSPA P320 Series 5 Centralog HMI & Controcad softwares, **All versions** **Applicable to Controcad in Controgen HX**	**Product based on Microsoft Windows XP Operating System** No Microsoft Windows patch available Our recommendation is first to apply defense in depth strategy to reduce the risk, including disconnect the system to all ethernet external network communication and then to implement Rip & Replace of the system.
ALSPA Series 6 MFC Controller	Analysis to define the best solution is still on going.
- Patch Management Station - Jump Station - Security Remote connection - Alspa Anti-Malware Antivirus Si - Back Up & Restore.	**We recommend customer to contact us to subscribe to an update of the product.**
Mark Vie Control ST software	Analysis to define the best solution is still on going.

As For these affected products we are still under evaluation to determine the impact of the corrective patch from Microsoft.
We strongly recommend you check that there is al defense in depth security measure.

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 Control System.
- 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 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	February 17, 2023	Initial version