GE
Steam Power
Automation & Controls

November 20th, 2020 **CYBERSECURITY** **ALSPA HMI & CCAD**

Topic: vulnerabilities “CVE2020-1472 “In Windows server OS station with AD functionality

Dear Valued Customer,

The following vulnerabilities in our Windows server OS station with AD functionality, an attacker could exploit the vulnerability thought network with a Net logon with an "ANONYMOUS LOGON" from somebody connected to the network domain. A successful exploit will lead to privilege escalation to domain administrator.

Details of these vulnerabilities are available from US-CERT in the following link
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

The product affected are:
- Domain controller Windows Server OS station

We have identified that the system we have provided to you has potentially one of these products and can be affected by this vulnerability.

We strongly recommend you check that there is no access to the domain controlled by the AD server from an illegitimate equipment.

Defense in depth

To minimize the risk of exposure to vulnerability’s, GE recommend implementing defense in depth strategy for critical process control system. If defense in depth is already in place we also strongly recommend you check that there is no loophole in the Access process to the legitimate equipment.

GE Power Automation & Control Contact information

We will be please to support the enhancement of the cyber security of your equipment with improved solution. 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 for cybersecurity services.

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