CYLON® TECHNICAL BULLETIN NO. 518
Issue Date: 09 June 2023

ASPECT® Security Improvements

Summary

CVE-2023-0635 and CVE-2023-0636 have been identified as vulnerabilities in ASPECT, specifically the administrative interface. These vulnerabilities are removed as of v `3.07.01`. These vulnerabilities are not exposed in a properly configured system.

Features

CVE-2023-0635 and CVE-2023-0636 have been identified as vulnerabilities in ASPECT, specifically the administrative interface. **You should refer to ABB document 2CKA000073B5403 for more detailed information regarding these vulnerabilities and workarounds**. Also refer to ABB document HT0045 Rev 6 regarding best network security practices with ABB controllers. Both documents can be found in ABB Library.

These vulnerabilities were identified when the administrative interface of ASPECT was left unconfigured and placed internet facing. As of 3.07.01, these vulnerabilities were retested in conjunction with Prism Infosec who is the security evaluator. (Find article High-risk vulnerability patched in ABB ASPECT Building Management System) These vulnerabilities no longer exist.

Never place unconfigured systems as internet facing. Take all precautions to avoid exposing ASPECT (or any other web server) needlessly in positions where they may be vulnerable. Ensure BMS networks are secure, passwords are routinely changed, and software has been updated.

Customer Impact

If your system is properly secure such that the administrative interface to ASPECT is not accessible, there is no impact to you. ABB encourages diligence in updating to the most current version of ASPECT for the latest security and features.

B0353 rev 1