ABB CYLON® TECHNICAL BULLETIN NO. 545
Issue Date: 03 December 2024

ASPECT® v3.08.03

Summary

The ASPECT v`3.08.03` release includes a wide range of security improvements. These improvements result from rigorous security assessments and significantly strengthen ASPECT against potential threats.

Detail

DON'T EXPOSE YOUR DEVICES ON THE INTERNET

Although a comprehensive discussion of network security is far beyond the scope of this document, the following items provide a starting point for creating a secure equipment installation. Where available, users should always defer to the security policies of the hosting network organization.

1. Always ensure that the ABB Cylon® Building Energy Management System (BEMS) solution is deployed on an isolated network specifically designated for BEMS controls only, with no connections to external networks.
2. Strictly prohibit the connection of ABB Cylon® BEMS devices to networks that include security-critical IP devices, such as CCTV systems, any data-sensitive infrastructure or credit card terminals.
3. ABB Cylon® BEMS solutions should never be exposed to the Internet. Exposure turns your system into a potential target accessible by every individual and machine globally.
4. Adopt a zero-exposure policy for ABB Cylon® devices on the internet. Always prioritize security by limiting information exposure to the minimum necessary for operational functionality.
5. Mandate the use of Secure Virtual Private Networks (VPNs) for all remote access requirements and always employ a Firewall for services requiring internet connectivity. VPNs ensure that devices remain off the public internet while providing a secure and encrypted path for authorized users to access system functions.

For more details see HT0038 ASPECT, FBXi and CBXi System Network Security Best Practice

INSTALLATION

Note: **ABB recommends closing all unnecessary ports on an ASPECT device.
After upgrading, always review port configuration for any unnecessarily open ports and close them accordingly.**

To take advantage of product enhancements and resolutions in ASPECT v`3.08.03`, you must upgrade the firmware of your existing ASPECT target (MATRIX Series, NEXUS Series, ASPECT-Enterprise) using the `System Update` feature within the target's `WebUI`.

Instructions on this process can be found in the ASPECT-Studio Online Help anytime. Once your target's firmware has been updated, you must open your existing project using ASPECT-Studio v`3.08.03`, perform a Clean and then deploy your project to the target. This process must be done to ensure that your project files receive all enhancements and that updated drivers are included as part of this maintenance release.

SECURITY IMPROVEMENTS

ASP-6825 Remove sensitive data from all request headers (Basic Auth), cookies and payload data in `ngAdmin` and `WebUI`.

ASP-6903 Prevent plain-text credentials from being passed from `ngAdmin` to the ASPECT server.

ASP-7012 Examine other places where unencrypted credentials are being passed in requests (`Change Password`, `Edit Auth`, etc.).

ASP-6297 Add facility to increase the number of TLS ciphers supported on targets with older Java versions.

ASP-6585 Add HTTP interceptor to `ngAdmin` to mitigate XSS vulnerabilities.

ASP-6774 Implement Session Timeout features for LDAP.

ASP-6775 Implement group-based access restrictions for LDAP users in `ngAdmin.`

ASP-7116 Apply latest OS patches for known CVEs.

ASP-6897 Fix NWS Weather service on MATRIX (by enhancing SSL cipher support).

ASP-7018 Apply encrypted-checksum security measure to BSX uploads directly from ASPECT-Studio.

ASP-6568 Improve support for standard punctuation characters in passwords.

CVEs MITIGATED

CVE-2024-6515 Web browser interface may manipulate application username/password in clear text or Base64 encoding in ABB ASPECT providing a higher probability of unintended credentials exposure. <=`3.08.02`

CVE-2024-6516 Cross Site Scripting vulnerabilities where found in ABB ASPECT providing a potential for malicious scripts to be injected into a client browser. <=`3.08.02`.

CVE-2024-6784 Server-Side Request Forgery vulnerabilities were found in ASPECT providing a potential for access to unauthorized resources and unintended information disclosure. <=`3.08.02`.

CVE-2024-48843 SQL injection vulnerabilities where found in ASPECT providing a potential for unintended information disclosure. This issue affects ASPECT <=`3.08.02`.

CVE-2024-48844 Denial of Service vulnerabilities where found in ASPECT providing a potential for device service disruptions. This issue affects ASPECT <=`3.08.02`.

CVE-2024-48845 Weak Password Reset Rules vulnerabilities where found in ASPECT providing a potential for the storage of weak passwords that could facilitate unauthorized admin/application access. This issue affects ASPECT <=`3.07.02`.

CVE-2024-48846 Cross Site Request Forgery vulnerabilities where found in ASPECT providing a potential for exposing sensitive information or changing system settings. This issue affects ASPECT <=`3.08.02`.

CVE-2024-48847 MD5 Checksum Bypass vulnerabilities where found in ASPECT exploiting a weakness in the way an application dependency calculates or validates MD5 checksum hashes. This issue affects ASPECT <= `3.08.01`.

CVE-2024-48839 Improper Input Validation vulnerability in ASPECT allows Remote Code Execution. This issue affects ASPECT <=`3.08.02`.

CVE-2024-48840 Unauthorized Access vulnerabilities in ASPECT allow Remote Code Execution. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51541 Local File Inclusion vulnerabilities in ASPECT allow access to sensitive system information. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51542 Configuration Download vulnerabilities in ASPECT allow access to dependency configuration information. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51543 Information Disclosure vulnerabilities in ASPECT allow access to application configuration information. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51544 Service Control vulnerabilities in ASPECT allow access to service restart requests and VM configuration settings. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51545 Username Enumeration vulnerabilities ASPECT allow access to application level username `add`, `delete`, `modify` and `list` functions. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51546 Credentials Disclosure vulnerabilities in ASPECT allow access to on board project backup bundles. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51548 Dangerous File Upload vulnerabilities in ASPECT allow upload of malicious scripts. This issue affects ASPECT <= `3.08.02`.

Subject to change without notice

CVE-2024-51549 Absolute File Traversal vulnerabilities in ASPECT allows access and modification of unintended resources. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51550 Data Validation / Data Sanitization vulnerabilities in ASPECT Linux allows unvalidated and unsanitized data to be injected in an Aspect device. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51551 Default Credential vulnerabilities in ASPECT on Linux allows access to an ASPECT device using publicly available default credentials. This issue affects ASPECT <= through `3.07.02`.

CVE-2024-51554 Off By One Error vulnerabilities in ASPECT allow an array out of bounds condition in a log script. This issue affects ASPECT <= `3.08.02`.

CVE-2024-51555 Default Credential vulnerabilities in ASPECT allows access to an ASPECT device using publicly available default credentials since the system does not require the installer to change default credentials. This issue affects ASPECT<= `3.07.02`.

CVE-2024-11316 Filesize Check vulnerabilities in ASPECT allow a malicious user to bypass size limits or overload an ASPECT device. This issue affects ASPECT <= `3.08.02`.

CVE-2024-11317 Session Fixation vulnerabilities in ASPECT allow an attacker to fix a user session identifier before login providing an opportunity for session takeover on an Aspect device. This issue affects ASPECT <= `3.08.02`.

GENERAL USABILITY IMPROVEMENTS

ASP-7020 Add a utility to apply a software patch to an ASPECT target from ASPECT-Studio.

ASP-6907 Improve touchscreen performance on eXplorer devices.

ASP-7255 Patch Day 1 bug when Modbus RTU is enabled on 2 ports.

ASP-6784 Fix NEXUS factory reset script to reset usernames and passwords to default values.

ASP-6989 Change the license server to allow `750` points for a MATRIX-11 / MATRIX-2-11.

ASP-7093 Remove onboard Calendaring Configuration option from the WebUI menu (ASPECT-Enterprise/NEXUS/MATRIX).

ASP-7132 Improve support for large project deployment to MATRIX devices (LW and ASPECT).

ASP-6614 Resolve a bug in WebUI Groups page which occurs when a group has no members.

DEPRECATED FEATURES

The following features in ASPECT have been deprecated to enhance security and increase usability of the product:

"Calendar Configuration" section in WebUI.

Customer Impact

Users **must upgrade as soon as possible** to ensure their ASPECT targets are secure and to take advantage of the latest features and improvements.

Note: ASPECT is not designed to be an "internet-facing" server application. If you need to access the ASPECT device remotely, you should do so through a secure VPN (and not a publicly accessible internet domain).

Note: ABB recommends that all ports other than https (`443`) are closed on an ASPECT device.
After upgrading, always review port configuration (WebUI > Communication Setup > IP Port Administration) for any unnecessarily open ports and close accordingly.

Note: It is recommended that `.aam` file checksums are verified against those published on the online ToolBox before a System Upgrade is performed.

Note: If you have any difficulty accessing ASPECT after upgrade, you may need to:

1. Clear your browsers history/cookies and restart the browser to clear out the older version/data (performing a hard refresh with Ctrl+F5 is an alternative option).
2. If login is still not working after clearing the cache, you may need to use the alternative WebUI login page at `https://192.168.0.1/altlogin.php` (replace the IP with your device's host/IP).