DOCUMENT ID: 7PAA020047
REVISION: C
DATE: 2026-06-16

CYBER SECURITY ADVISORY

Advant Master Online Builder DLL vulnerability

CVE ID: CVE-2025-13162

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations (e.g. ICS-CERT).

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

- Control Builder A versions 1.4/4 and earlier
- ABB 800xA for Advant Master versions 6.0.3-1 and earlier
- ABB 800xA for Advant Master versions 6.1.1-1 and earlier
- ABB 800xA for Advant Master version 6.1.1-3
- ABB 800xA for Advant Master version 6.2.0-1

Vulnerability IDs and Product Issue Numbers (PIN)

Vulnerability ID : CVE-2025-13162

PIN: PIN-2M5AY2

Summary

ABB has become aware of a vulnerability in the product versions listed above, where an incorrect version of Online Builder (ONB) was included in the media.

An update is available that resolves the vulnerability, see details in *Recommended immediate actions* below.

Recommended immediate actions

ABB has investigated vulnerability and remediated it in the newly released versions. The vulnerability has been resolved in the product versions listed below:

Product	Version	Recommended action
Control Builder A	Versions 1.4/4 and earlier	Update to version 1.4/5 or later
800xA for Advant Master	Versions 6.0.3-1 and earlier	Update to version 6.1.1-5 or later
800xA for Advant Master	Versions 6.1.1-1 and earlier	Update to version 6.1.1-5 or later
800xA for Advant Master	Versions 6.1.1-2 [1]	Update to version 6.1.1-5 or later
800xA for Advant Master	Version 6.1.1-3 [1]	Update to version 6.1.1-5 or later
800xA for Advant Master	Version 6.1.1-4 [2]	Update to version 6.1.1-5 or later
800xA for Advant Master	Version 6.2.0-1	Update to version 6.2.0-3 or later
800xA for Advant Master	Version 6.2.0-2 [3]	Update to version 6.2.0-3 or later

[1] Version 6.1.1-2 does not contain this vulnerability and therefore no update is required. The vulnerability was again introduced in 6.1.1-3 when an older ONB version was included in the release media.

[2] Version 6.1.1-4 do not contain this vulnerability but present version 6.1.1-3 by 800xA System Installer and System Configuration Console (SCC). Version 6.1.1-4 is therefore withdrawn.

[3] Version 6.2.0-2 do not contain this vulnerability but present version 6.2.0-1 by 800xA System Installer and System Configuration Console (SCC). Version 6.2.0-2 is therefore withdrawn.

ABB recommends that customers apply the update at their earliest convenience.

Vulnerability, severity and details

A vulnerability exists in the Online Builder (ONB) version included in the product versions listed above.

The application improperly handles the search path for loading DLL´s, potentially allowing unauthorized libraries from untrusted directories. An attacker who obtains the necessary access could exploit the vulnerability leading to unauthorized code execution and compromising system integrity.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

CVE-2025-13162 Advant Master Online Builder DLL vulnerability

The application improperly handles the search path for loading DLL´s, potentially allowing unauthorized libraries from untrusted directories. An attacker who obtains the necessary access could exploit the vulnerability leading to unauthorized code execution and compromising system integrity.

CVSS
CVSS v3.1 Base Score: 4.4 / Medium
CVSS v3.1 Temporal Score: 4.4 / Medium
Common Vulnerability Scoring System Version 3.1 Calculator
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:N

CVSS v4.0 Score: 4.1 / Medium
Common Vulnerability Scoring System Version 4.0 Calculator
CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:P/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

CWE
CWE-427: Uncontrolled Search Path Element

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-13162

Mitigating factors

Since it is required that the attacker has access to the system, it is important that all users that have access to the system are managed as recommended by ABB guidelines.

- Allow only authorized users to log on to the system and enforce strong passwords that are changed regularly.

[1] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[2] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

[3] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

[4] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

- Restrict temporary connection of portable computers, USB memory devices and other removable data carriers. Computers that can be physically accessed by regular users should have ports for removable data carriers disabled or at least managed to only allow intended device types.

For more information on recommended practices, see [1].

Workarounds

The recommendation is to upgrade to a version where the vulnerability is corrected. If an upgrade Is not possible and a workaround is needed, contact ABB Support.

Frequently asked questions

What is the scope of vulnerability?

An attacker who successfully exploited this vulnerability could insert and run arbitrary code in an affected system node.

What causes the vulnerability?

The vulnerability is caused by not having restricted permission on an application directory where DLL files are stored.

What is Advant Master Online Builder?

Online Builder is part of Control Builder A, being a set of applications for configuration and programming of Advant Master controllers.
Online Builder is also part of 800xA for Advant Master, an extension package to System 800xA connecting to Advant Master controllers.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability can run arbitrary code in an affected node.

How could an attacker exploit the vulnerability?

An attacker who obtains the necessary access could exploit vulnerability by placing malicious DLL´s in the unrestricted application directory, leading to unauthorized code execution and compromising system integrity.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have physical access to an affected system node.

Can functional safety be affected by an exploit of this vulnerability?

No.

What does the update do?

The update of the Online Builder (ONB) resolves the vulnerability by adding restrictions to the application folder, requiring authentication.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, ABB identified this vulnerability through its internal security assessment and verification processes.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

General security recommendations

Control systems and the control network are exposed to cyber threats. To minimize these risks, the protective measures and best practices listed below are available in addition to other measures. ABB strongly recommends system integrators and asset owners to implement the measures they consider appropriate for their control system environment:

- Place control systems in a dedicated control network containing control systems only.
- Locate control networks and systems behind firewalls and separate them from any other networks like business networks and the Internet.
- Block any inbound Internet traffic destined for the control networks/systems. Place remote access systems used for remote control system access outside the control network.
- Limit outbound Internet traffic originating from control systems/networks as much as possible. If control systems must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which control systems need to use for normal control operation.
- If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.
- Limit exposure of control networks/systems to internal systems. Tailor firewall rules allowing traffic from internal systems to control networks/systems to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal control operation.
- Create strict firewall rules to filter malicious network traffic targeting control system vulnerabilities ("exploit traffic"). Exploit traffic may use network communication features like source routing, IP fragmentation and/or IP tunneling. If such features are not required for normal control operation, block them on your firewall.
- If supported by your firewall, apply additional filters to allowed traffic which provide protection for control networks/systems. Such filters are provided by advanced firewall features like Application Control and Anti-Virus.
- Use Intrusion Detection Systems (IDS) or Intrusion Preventions Systems (IPS) to detect/block control system-specific exploit traffic. Consider using IPS rules protecting against control system exploits.

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please ensure that VPN solutions are updated to the most current version available.
- In case you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.
- Harden your control systems by enabling only the ports, services and software required for normal control operation. Disable all other ports and disable/uninstall all other services and software.
- If possible, limit the permissions of user accounts, software processes and devices to the permissions required for normal control operation.
- Use trusted, patched software and malware protection solutions. Interact with trusted web sites and trusted email attachments only.
- Ensure all nodes are always up to date in terms of installed software, operating system and firmware patches as well as anti-virus and firewall.
- Protect control systems from physical access by unauthorized personnel e.g. by placing them in locked switch cabinets.

Support

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Revision history

Rev. Ind.	Page (P) Chapter (C)	Change description	Rev. date
A	all	WITHDRAWN	2026-01-14
B	All	New version	2026-03-20
C	Chapter: “Recommended immediate actions”	Changed from recommended version 6.1.1-4 to 6.1.1-5 and from recommended version 6.2.0-2 to 6.2.0-3	2026-06-11