DOCUMENT ID: 7PAA022088
REVISION: B
DATE: 2025-11-20

CYBER SECURITY ADVISORY

Edgenius Management Portal Authentication Bypass
ABB Ability Edgenius
CVE ID: CVE-2025-10571

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

Product Name	Product Version
ABB Ability Edgenius	3.2.0.0
ABB Ability Edgenius	3.2.1.1

Vulnerability IDs

CVE-2025-10571

Summary

ABB identified a critical vulnerability present in versions 3.2.0.0 and 3.2.1.1 of ABB Ability Edgenius. We have not received any reports of this vulnerability being exploited.

An unauthenticated attacker could exploit this vulnerability to:

- → install and run arbitrary code,
- → uninstall installed applications,
- → modify the configuration of installed applications,

on systems running the vulnerable versions of ABB Ability Edgenius.

Recommended immediate actions

ABB has prepared an update to fix this vulnerability included in the latest Roll-Up, **ABB Ability Edgenius version 3.2.2.0.**

ABB advises customers to upgrade as soon as possible. Until the upgrade is applied, ABB advises customers to **disable the Edgenius Management Portal** to mitigate the vulnerability.

Vulnerability severity and details

The Edgenius Management Portal in the affected product versions contains a vulnerability that allows authentication to be bypassed. An attacker could exploit the vulnerability by sending a specially crafted message to the system node allowing the attacker to install and run arbitrary code, uninstall installed applications and modify the configuration of installed applications.

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-2025-10571 ABB Ability Edgenius Authentication Bypass

ABB Ability Edgenius versions 3.2.0.0 and 3.2.1.1 contain a critical authentication bypass vulnerability.

CVSS

CVSS v3.1 Base Score:	9.6
CVSS v3.1 Temporal Score:	9.0
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:T/RC:C
CVSS v4.0 Score:	9.4
CVSS v4.0 Vector:	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

CWE

CWE-288: Authentication Bypass Using an Alternate Path or Channel

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-10571

[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/.

Mitigating factors

Exploitation requires an attacker to have gained access to the network where Edgenius has been deployed, and while the Edgenius Management Portal is running.

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Workarounds

Workarounds are specific measures that a user can take to help block an attack, for example, temporarily disabling the vulnerable feature may remove the exposure with well-known impact on functionality. ABB has tested the following workaround.

Disabling the Edgenius Management Portal will disable the vulnerable component. This will have no impact on the day-to-day operations of an already deployed and configured system. Refer to the CVE-2025-10571 Workaround Instructions (7PAA022086*), distributed separately.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could install and run arbitrary code, uninstall installed applications and modify the configuration of installed applications.

What causes the vulnerability?

The vulnerability is caused by an underlying API (Application Programming Interface) not adequately verifying authentication.

What is ABB Ability Edgenius Management Portal?

ABB Ability Edgenius Management Portal allows administrators to configure their edge and manage applications.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could be able to run arbitrary code on the edge and modify the configuration of installed applications.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct

connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?

The update removes the vulnerability, ensuring that the vulnerable parts of the Edgenius Management Portal validate authorization for requests.

Meanwhile please refer to the defined mitigations and workaround.

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

No, ABB discovered this vulnerability through internal testing.

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.

References

7PAA022086_en	CVE-2025-10571 Workaround Instructions

Support

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

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

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
B	all	Initial version	2025-11-20