CYBER SECURITY ADVISORY

Busch-Welcome® 2 wire
Door opener actuator by default in compatibility mode.

CVE ID: CVE-2025-7705

Notice

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.

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

Platform	Model number	ABB Product ID	Affected firmware Version
Switch Actuator 4 DU	83330	2CKA008300A0044	All
Switch actuator, door/light 4 DU	83330-500	2TMA020110N0003	All

Note: All the Platforms listed above are defined as WELCOME_DOOR_ACTUATOR in the subsequent document.

Vulnerability IDs

No.	CVE ID	Title	Affected SW version
1	CVE-2025-7705	Authentication bypass due to compatibility mode enabled by default	All

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above due to a misconfiguration during production. A procedure to resolve this misconfiguration is delivered with this document.

An attacker who successfully exploited this vulnerability could gain physical, unauthorized access to a Building where the product is installed.

Recommended immediate actions

ABB has analyzed this vulnerability and has concluded that a simple action on customer side will resolve it to its full extent.

The following actions need to be executed on premise where the respective Busch-Welcome® System is installed:

- While the Busch-Welcome® System is in operation, toggle the mode switch on the product from "Door-Open" - to "Light" – Mode, wait one second and switch back to "Door-Open" - Mode.
- Restart the Busch-Welcome® System with a Power reset (mains power off and on again).

By executing the above steps, the system will re-calibrate itself during boot up and will correct the misconfiguration automatically.

ABB recommends that customers apply the above-listed actions at the earliest convenience.

Vulnerability, severity and details

An attacker who successfully exploited this vulnerability, may be able to gain access to the building where a Busch-Welcome® two wire system is installed.

No.	CVE ID	Title	
1	CVE-2025-7705	Authentication bypass due to compatibility mode enabled by default	
	Source	Researcher	
	Status	Fixed	
	Description	A misconfiguration during production leads to a vulnerability in the door opener actuator device.	
	CWE	CWE-489:Active Debug Code	
	CVSS v3.1	Base Score:	6.8
		Temporal Score:	6.8
		Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	CVSS v4.0	Score	8.6
		Vector:	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-7705	

Mitigating factors

ABB recommends double check the system handbook of a Busch-Welcome® two wire system regarding security advises for the correct installation.

Frequently asked questions

What causes the vulnerability?

The WELCOME_DOOR_ACTUATOR setup into a compatibility mode at the end of production line. The vulnerability occurs because the compatibility mode remains after the production process is completed. This way the product is shipped to the customer with the compatibility mode enabled.

What is WELCOME_DOOR_ACTUATOR?

The intended use of the WELCOME_DOOR_ACTUATOR is to either switch on a light at the front door of a building or trigger the door opener on request of the resident. The product in scope of this advisory is only required if a building has more than one entry door, e.g. a front door and a second door at the back of the building. Most installations work with only one door open actuator which ships as standard feature of the central unit. The door open function of the central unit is not affected by this vulnerability.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could gain unauthorized access to a building where the product is installed and operating in its compatibility mode. The product is intended to extend a Busch-Welcome® system to support more then one entry door to the building. As the intended use of the Busch-Welcome® two wire system focuses on residential buildings, the customer demand to add a second entry door to the Busch-Welcome® system, seen rare.

Could the vulnerability be exploited remotely?

No, an attacker who aims to exploit this vulnerability need physical access to the facility where the Busch-Welcome® two wire system is installed.

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

The Busch-Welcome® two wire system does not support functional safety. The system is designed in a way that it is ensured that leaving the building is possible under any condition even in the event of mains power dropout.

What do the recommended intermediate actions do?

The recommended intermediate actions ensure that the device configuration returns to its intended default configuration.

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

No, ABB received information about this vulnerability through responsible disclosure.

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

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

– Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).

- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any net-work other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- 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.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

More information on recommended practices can be found in the following documents:

9AKK106713A5111 Guide for network security in building systems control

References

9AKK106713A5111 Guide for network security in building systems control

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
A	all	Initial version	

